IFCT0109. SEGURIDAD INFORMÁTICA

MF0490_3 GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UD07

ADMINISTRACIÓN DEL CONTROL DE ACCESOS ADECUADOS DE LOS SISTEMAS DE INFORMACIÓN

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

1. INTRODUCCIÓN

CUANDO SE HABLA DE SERVICIOS EN EL SISTEMA INFORMÁTICO, NO HAY QUE OLVIDAR EL TEMA DE LA **SEGURIDAD**.

UN SISTEMA INFORMÁTICO MAL PROTEGIDO PUEDE PONER EN PELIGRO LOS DATOS QUE CONTIENE Y SE PUEDE INCURRIR INCLUSO EN PROBLEMAS LEGALES, PRODUCIENDO **GRAVES DAÑOS Y COSTES A LAS ORGANIZACIONES**.

ES FUNDAMENTAL QUE LAS ORGANIZACIONES ESTABLEZCAN POLÍTICAS DE SEGURIDAD QUE IMPIDAN LA UTILIZACIÓN MALINTENCIONADA DE LOS RECURSOS Y CUALQUIER TIPO DE INCIDENCIA QUE PUEDA OCURRIR POR LA FALTA DE PROTECCIÓN DEL SISTEMA.

1. INTRODUCCIÓN

UNA MEDIDA DE SEGURIDAD IMPRESCINDIBLE ES LA REFERENTE AL **CONTROL DE ACCESOS.**

SE DEBE DISEÑAR UN SISTEMA DE CONTROL DE ACCESOS QUE PERMITA QUE **CADA USUARIO SOLO TENGA ACCESO A LOS ARCHIVOS ESTRICTAMENTE NECESARIOS PARA EL DESARROLLO DE SUS FUNCIONES** Y QUE, ADEMÁS, SOLO PUEDA HACER UNA SERIE DE ACCIONES LIMITADAS CON ELLOS.

CONTENIDOS

1. INTRODUCCIÓN
2. **ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS**
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

LOS PRINCIPALES REQUERIMIENTOS DE ACCESO DE LOS SISTEMAS DE INFORMACIÓN Y DE LOS RECURSOS COMPARTIDOS SE ENCUENTRAN RECOGIDOS PRINCIPALMENTE EN LA NORMATIVA **ISO/IEC 27002**

LA PARTE REFERENTE AL CONTROL DE ACCESOS SE LOCALIZA EN EL APARTADO **9** DE DICHA NORMATIVA

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

LA PRINCIPAL FINALIDAD DEL ESTABLECIMIENTO DEL **CONTROL DE ACCESOS** EN UNA ORGANIZACIÓN **ES CONTROLAR EL ACCESO A LA INFORMACIÓN**, TANTO EXTERNO COMO INTERNO.

UNA BUENA PRÁCTICA RECOMENDADA POR LA NORMATIVA ES EL **ESTABLECIMIENTO DE UNA POLÍTICA DE CONTROL DE ACCESOS ADECUADA Y DOCUMENTADA, ADEMÁS DE SU REVISIÓN PERIÓDICA.**

EN ESTA POLÍTICA DE CONTROL DE ACCESOS DEBEN ESTABLECERSE LAS REGLAS DE CONTROL DE ACCESO Y LOS DERECHOS PARA CADA USUARIO O GRUPO DE USUARIOS

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

HAY QUE TENER EN CUENTA LOS SIGUIENTES ELEMENTOS:

- LOS REQUERIMIENTOS DE SEGURIDAD DE LAS APLICACIONES COMERCIALES INDIVIDUALES.
- LA IDENTIFICACIÓN DE TODA LA INFORMACIÓN RELACIONADA CON LAS APLICACIONES COMERCIALES Y LOS RIESGOS QUE ENFRENTA LA INFORMACIÓN.
- LAS POLÍTICAS PARA LA DIVULGACIÓN Y AUTORIZACIÓN DE LA INFORMACIÓN.
- LA CONSISTENCIA ENTRE EL CONTROL DE ACCESOS Y LAS POLÍTICAS DE CLASIFICACIÓN DE LA INFORMACIÓN DE LOS DIFERENTES SISTEMAS Y REDES.
- LA LEGISLACIÓN RELEVANTE Y CUALQUIER OBLIGACIÓN CONTRACTUAL RELACIONADA CON LA PROTECCIÓN DEL ACCESO A LOS DATOS O A LOS SERVICIOS.

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

- LOS PERFILES DE ACCESO DE USUARIO ESTÁNDAR PARA PUESTOS DE TRABAJO COMUNES EN LA ORGANIZACIÓN.
- LA GESTIÓN DE LOS DERECHOS DE ACCESO EN UN AMBIENTE DISTRIBUIDO Y EN RED QUE RECONOCE TODOS LOS TIPOS DE CONEXIONES DISPONIBLES.
- LA SEGREGACIÓN DE LOS ROLES DEL CONTROL DE ACCESOS.
- LOS REQUERIMIENTOS PARA LA AUTORIZACIÓN FORMAL DE LAS SOLICITUDES DE ACCESO.
- LOS REQUERIMIENTOS PARA LA REVISIÓN PERIÓDICA DE LOS CONTROLES DE ACCESO.
- LA REVOCACIÓN DE LOS DERECHOS DE ACCESO.

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

EN EL MOMENTO DE ESPECIFICAR LOS CONTROLES DE ACCESO ES NECESARIO **ESTABLECER UNA SERIE DE PARÁMETROS**:

- DIFERENCIACIÓN ENTRE LAS REGLAS DE OBLIGATORIO CUMPLIMIENTO Y LOS LINEAMIENTOS QUE SON DE CUMPLIMIENTO RECOMENDADO PERO OPCIONAL.
- ESTABLECIMIENTO DE LAS REGLAS BASADAS EN LA PREMISA: “GENERALMENTE TODO ESTÁ PROHIBIDO A NO SER QUE ESTÉ EXPRESAMENTE PERMITIDO”.
- CAMBIOS EN LOS PROCESOS DE IDENTIFICACIÓN DE LA INFORMACIÓN QUE SE INICIAN DE MODO AUTOMÁTICO MEDIANTE LOS MEDIOS DE TRATAMIENTO DE LA INFORMACIÓN Y AQUELLOS QUE SE INICIAN DE MODO MANUAL POR UN ADMINISTRADOR.
- CAMBIOS EN LOS PERMISOS DE USUARIOS QUE SE INICIAN AUTOMÁTICAMENTE POR EL SISTEMA DE INFORMACIÓN O DE FORMA MANUAL POR EL ADMINISTRADOR.
- REGLAS QUE REQUIEREN LA APROBACIÓN ESPECÍFICA ANTES DE PROMULGARSE Y AQUELLAS QUE NO LA REQUIEREN.

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

OTROS PUNTOS IMPORTANTES SOBRE EL CONTROL DE ACCESOS EN ISO 27002

LOS PRINCIPALES **REQUERIMIENTOS** PARA QUE LA ORGANIZACIÓN DISEÑE UNA POLÍTICA CORRECTA DE CONTROL DE ACCESOS SON:

- **GESTIÓN DE ACCESO DEL USUARIO**

  HAY QUE ASEGURAR QUE EL ACCESO SOLO SEA PARA LOS USUARIOS AUTORIZADOS Y EVITAR QUE LOS NO AUTORIZADOS PUEDAN ACCEDER A LOS SISTEMAS DE INFORMACIÓN.

- **RESPONSABILIDADES DEL USUARIO**

  HAY QUE EVITAR EL ACCESO DE USUARIOS NO AUTORIZADOS, EVITANDO ASÍ PONER EN PELIGRO LA INFORMACIÓN Y EL ROBO DE LA MISMA Y DE SUS MEDIOS DE PROCESAMIENTO.

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

OTROS PUNTOS IMPORTANTES SOBRE EL CONTROL DE ACCESOS EN ISO 27002

- **CONTROL DE ACCESO A LA RED**

  HAY QUE EVITAR EL ACCESO DE LOS USUARIOS NO AUTORIZADOS A LOS SERVICIOS DE REDES, TANTO INTERNAS COMO EXTERNAS, PARA NO COMPROMETER SU SEGURIDAD.

- **CONTROLAR LOS ACCESOS AL SISTEMA OPERATIVO PARA EVITAR ACCESOS NO AUTORIZADOS**

  SE RECOMIENDA UTILIZAR MEDIOS DE SEGURIDAD QUE PERMITAN AUTENTICAR A LOS USUARIOS AUTORIZADOS, REGISTRAR LOS INTENTOS DE ACCESO Y LA UTILIZACIÓN DE PRIVILEGIOS ESPECIALES

2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS

OTROS PUNTOS IMPORTANTES SOBRE EL CONTROL DE ACCESOS EN ISO 27002

- **CONTROL DE ACCESO A LA APLICACIÓN Y LA INFORMACIÓN**

  SE DEBEN UTILIZAR MEDIOS DE SEGURIDAD QUE RESTRINJAN EL ACCESO A LAS APLICACIONES Y SU UTILIZACIÓN PARA EVITAR ACCESOS NO AUTORIZADOS.

- **INFORMÁTICA MÓVIL Y TELETRABAJO**

  HAY QUE GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN EN EL USO DE RECURSOS DE INFORMÁTICA MÓVIL Y TELETRABAJO.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. **PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS**
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

EN EL APARTADO **9.2** DE LA **ISO/IEC 27002** SE ENUMERAN ESTOS PRINCIPIOS Y BUENAS PRÁCTICAS, DIFERENCIANDO ENTRE:

- **REGISTRO Y BAJA DEL USUARIO**
- **GESTIÓN DE PRIVILEGIOS DE ACCESO**
- **GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS**
- **REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO**

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

REGISTRO Y BAJA DEL USUARIO

EN LAS ORGANIZACIONES **DEBE HABER ESTABLECIDO UN PROCEDIMIENTO FORMAL PARA EL REGISTRO Y LA ELIMINACIÓN DEL REGISTRO DEL USUARIO**, QUE PERMITA OTORGAR Y REVOCAR EL ACCESO A TODOS LOS SISTEMAS DE INFORMACIÓN DE LA ORGANIZACIÓN.

ESTE PROCEDIMIENTO FORMAL PARA EL REGISTRO DE USUARIOS DEBERÍA INCLUIR UNA SERIE DE **PRINCIPIOS**:

- **UTILIZAR IDENTIFICADORES (IDS) DE USUARIOS ÚNICOS**. LA UTILIZACIÓN DE IDENTIFICADORES GRUPALES DEBE LIMITARSE SOLO POR RAZONES COMERCIALES U OPERACIONALES, Y DEBEN SER APROBADOS Y DOCUMENTADOS BAJO CONSENSO.
- **COMPROBAR QUE EL USUARIO DISPONE DE LA AUTORIZACIÓN PARA EL USO DEL SISTEMA DE INFORMACIÓN.** TAMBIÉN SE RECOMIENDA UNA APROBACIÓN SEPARADA DE LA GERENCIA PARA LOS DERECHOS DE ACCESO.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

REGISTRO Y BAJA DEL USUARIO

- **COMPROBAR QUE EL NIVEL DE ACCESO OTORGADO AL USUARIO SEA EL ADECUADO** PARA EL PROPÓSITO MARCADO Y CONSISTENTE CON LA POLÍTICA DE SEGURIDAD DEFINIDA EN LA ORGANIZACIÓN.
- FACILITAR A LOS USUARIOS UN DOCUMENTO ESCRITO DONDE ESTÉN REFLEJADOS SUS DERECHOS DE ACCESO.
- REQUERIR A LOS USUARIOS SU FIRMA EN EL DOCUMENTO DONDE SE REFLEJAN SUS DERECHOS DE ACCESO PARA ACREDITAR QUE ENTIENDEN LOS ENUNCIADOS Y SUS DERECHOS.
- ASEGURAR QUE LOS PROVEEDORES NO FACILITEN EL ACCESO HASTA QUE NO SE HAYAN COMPLETADO TODOS LOS PROCESOS DE AUTORIZACIÓN.
- MANTENER UN REGISTRO FORMAL DE TODAS LAS PERSONAS AUTORIZADAS PARA UTILIZAR EL SISTEMA DE INFORMACIÓN.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

REGISTRO Y BAJA DEL USUARIO

- ELIMINAR O BLOQUEAR DE MODO INMEDIATO LOS DERECHOS DE ACCESO A LOS USUARIOS QUE HAN CAMBIADO DE PUESTO DE TRABAJO O QUE HAN DEJADO DE TRABAJAR PARA LA ORGANIZACIÓN.
- REALIZAR COMPROBACIONES PERIÓDICAS PARA ELIMINAR O BLOQUEAR IDENTIFICADORES DE USUARIO Y CUENTAS REDUNDANTES.
- ASEGURAR QUE NO SE EMITAN IDENTIFICADORES DE USUARIO REDUNDANTES A OTROS USUARIOS.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

GESTIÓN DE PRIVILEGIOS DE ACCESO

HAY QUE RESTRINGIR Y CONTROLAR ADECUADAMENTE LA ASIGNACIÓN Y EL USO DE LOS PRIVILEGIOS DE LA ORGANIZACIÓN.

EN LA DEFINICIÓN DE ESTE PROCEDIMIENTO FORMAL SE DEBE CONSIDERAR UNA SERIE DE **ELEMENTOS**:

- LOS PRIVILEGIOS DE ACCESO ASOCIADOS CON CADA ELEMENTO DISTINTO DEL SISTEMA DE INFORMACIÓN. POR EJEMPLO, ASIGNAR PRIVILEGIOS DE ACCESO DISTINTOS PARA CADA APLICACIÓN DEL SISTEMA.
- LOS PRIVILEGIOS DEBEN SER ASIGNADOS CONFORME AL PRINCIPIO: *LOS USUARIOS DEBEN ACCEDER A SOLO LO QUE DEBEN SABER*. ES DECIR, CADA USUARIO DEBE PODER ACCEDER SOLO A LO ESTRICTAMENTE NECESARIO PARA EL DESEMPEÑO DE SUS TAREAS.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

GESTIÓN DE PRIVILEGIOS DE ACCESO

- HAY QUE MANTENER ACTUALIZADO EL PROCEDIMIENTO DE AUTORIZACIÓN Y EL REGISTRO DE TODOS LOS PRIVILEGIOS QUE SE VAN ASIGNANDO. SE RECOMIENDA NO ASIGNAR PRIVILEGIOS HASTA QUE NO HA TERMINADO POR COMPLETO EL PROCEDIMIENTO DE AUTORIZACIÓN.
- HAY QUE PROMOVER EL DESARROLLO Y LA UTILIZACIÓN DE RUTINAS DEL SISTEMA PARA REDUCIR AL MÍNIMO LA NECESIDAD DE ASIGNAR PRIVILEGIOS PARA TAREAS BÁSICAS Y SISTEMÁTICAS.
- HAY QUE PROMOVER EL DESARROLLO Y LA UTILIZACIÓN DE AQUELLAS APLICACIONES QUE EVITEN LA NECESIDAD DE UTILIZAR PRIVILEGIOS.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

PARA LAS ORGANIZACIONES TAMBIÉN ES **FUNDAMENTAL ESTABLECER UN PROCEDIMIENTO FORMAL DE GESTIÓN PARA LA ASIGNACIÓN DE CONTRASEÑAS A LAS CUENTAS DE USUARIO**. ESTE PROCEDIMIENTO DEBE INCLUIR LO SIGUIENTE:

- HAY QUE REQUERIR QUE LOS USUARIOS FIRMEN UN DOCUMENTO PARA MANTENER LA CONFIDENCIALIDAD DE LAS CONTRASEÑAS Y TAMBIÉN PARA CONSERVAR LAS CLAVES GRUPALES SOLO DENTRO DE LOS MIEMBROS DEL GRUPO.
- A LOS USUARIOS SE LES DEBE ASIGNAR PRIMERAMENTE UNA CLAVE TEMPORAL SEGURA QUE DEBEN CAMBIAR INMEDIATAMENTE A UNA CONTRASEÑA SECRETA PROPIA.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

- HAY QUE ESTABLECER PROCEDIMIENTOS QUE VERIFIQUEN LA IDENTIDAD DE LOS USUARIOS ANTES DE FACILITARLES UNA CONTRASEÑA NUEVA, SUSTITUTA O TEMPORAL.
- LAS CONTRASEÑAS PROVISIONALES DEBEN FACILITARSE A LOS USUARIOS DE UN MODO SEGURO, EVITANDO LA UTILIZACIÓN DE CORREO ELECTRÓNICO DE TERCEROS O NO PROTEGIDOS PARA ELLO.
- LAS CONTRASEÑAS PROVISIONALES DEBEN SER ÚNICAS Y DIFÍCILES DE ADIVINAR.
- EN EL MOMENTO DE RECIBIR UNA CONTRASEÑA, LOS USUARIOS DEBEN RECONOCER DICHA RECEPCIÓN.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

GESTIÓN DE LA INFORMACIÓN SECRETA DE AUTENTICACIÓN DE LOS USUARIOS

- LAS CONTRASEÑAS NUNCA DEBEN ALMACENARSE EN LUGARES CARENTES DE PROTECCIÓN ADECUADA.
- LAS CONTRASEÑAS INICIALES FACILITADAS POR EL VENDEDOR DEBEN MODIFICARSE DESPUÉS DE LA INSTALACIÓN DEL SOFTWARE ADQUIRIDO.

LAS CONTRASEÑAS SIRVEN COMO MEDIO COMÚN PARA IDENTIFICAR Y DAR PERMISO A LOS USUARIOS ANTES DE ACCEDER A UN SISTEMA DE INFORMACIÓN. TAMBIÉN SE RECOMIENDA LA UTILIZACIÓN DE OTRAS ALTERNATIVAS TECNOLÓGICAS PARA IDENTIFICAR A LOS USUARIOS, COMO UTILIZACIÓN DE FIRMAS ELECTRÓNICAS O SISTEMAS DE VERIFICACIÓN DE HUELLAS DIGITALES, ENTRE OTRAS.

3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS

REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIO

LOS DIRECTIVOS Y GERENTES DE LA ORGANIZACIÓN **DEBEN ENCARGARSE DE LA REVISIÓN PERIÓDICA DE LOS DERECHOS DE ACCESO DE LOS USUARIOS** MEDIANTE, TAMBIÉN, UN PROCEDIMIENTO FORMAL QUE DEBE INCLUIR POR LO MENOS:

- LOS DERECHOS DE ACCESO DE LOS USUARIOS DEBEN SER REVISADOS PERIÓDICAMENTE Y DESPUÉS DE CUALQUIER CAMBIO EN LA SITUACIÓN DEL USUARIO (ASCENSO EN EL PUESTO DE TRABAJO, TERMINACIÓN DE LA RELACIÓN DEL EMPLEADO CON LA EMPRESA, ETC.).
- LOS DERECHOS DE ACCESO DEBEN REVISARSE Y REASIGNARSE TAMBIÉN CUANDO EL USUARIO CAMBIA DE UN PUESTO DE TRABAJO A OTRO DENTRO DE LA MISMA ORGANIZACIÓN (MÁXIMO CADA SEIS MESES).
- LAS AUTORIZACIONES PARA PRIVILEGIOS ESPECIALES DEBEN SER REVISADAS CON MÁS FRECUENCIA QUE LAS AUTORIZACIONES ESTÁNDAR (MÁXIMO CADA TRES MESES).
- HAY QUE MANTENER UN REGISTRO DE TODOS LOS CAMBIOS REALIZADOS EN LAS CUENTAS PRIVILEGIADAS A FIN DE LLEVAR UN CONTROL DE LAS MISMAS EN LAS REVISIONES PERIÓDICAS.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. **REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS**
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS

LOS REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y A LA ASIGNACIÓN DE PRIVILEGIOS QUE HAY QUE TENER EN CUENTA SE REFIEREN SOBRE TODO AL **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS UE 679/2016**

ESTABLECEN COMO PRINCIPIO FUNDAMENTAL LA GARANTÍA DE LAS TRES PROPIEDADES DE LA INFORMACIÓN, YA MENCIONADAS ANTERIORMENTE:

- **INTEGRIDAD:** LA INFORMACIÓN NO DEBE SUFRIR CAMBIOS NO DESEADOS.
- **CONFIDENCIALIDAD**: SOLO LOS USUARIOS AUTORIZADOS DEBEN PODER TENER ACCESO A LA INFORMACIÓN.
- **DISPONIBILIDAD:** LA INFORMACIÓN DEBE ESTAR DISPONIBLE SIEMPRE QUE LAS PERSONAS AUTORIZADAS LO REQUIERAN

4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS

LOS RESPONSABLES DEL FICHERO DEBEN ENCARGARSE DE **ADOPTAR E IMPLANTAR UNA SERIE DE MEDIDAS,** QUE PUEDEN SER:

MEDIDAS ORGANIZATIVAS

MEDIDAS CUYOS OBJETIVOS ESTÁN ENCAMINADOS AL ESTABLECIMIENTO DE PROCEDIMIENTOS, NORMAS, REGLAS Y ESTÁNDARES DE SEGURIDAD PARA PROTEGER LOS DATOS PERSONALES EN EL MOMENTO DE SU TRATAMIENTO.

MEDIDAS TÉCNICAS

MEDIDAS CUYOS OBJETIVOS ESTÁN ENCAMINADOS A MANTENER LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN CUANDO ESTA CONTIENE DATOS DE CARÁCTER PERSONAL. ESTAS MEDIDAS ESTÁN CLASIFICADAS EN FUNCIÓN DEL NIVEL DE SEGURIDAD DE SUS DATOS: **BÁSICO, MEDIO Y ALTO**.

4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS

NIVEL BÁSICO

ES UN FICHERO O TRATAMIENTO DE DATOS BÁSICO CUALQUIER OTRO FICHERO DISTINTO A LOS INDICADOS QUE CONTENGA DATOS DE CARÁCTER PERSONAL.

UNA DE LAS MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO (Y QUE, POR TANTO, DEBE IMPLANTARSE EN TODO TIPO DE FICHEROS AUTOMATIZADOS) ES QUE SE ESTABLEZCA UN PROCEDIMIENTO DE ASIGNACIÓN Y DISTRIBUCIÓN DE CONTRASEÑAS Y QUE LAS CONTRASEÑAS SE CAMBIEN, AL MENOS, UNA VEZ AL AÑO.

TAMBIÉN SE CONSIDERAN DE NIVEL BÁSICO LOS FICHEROS O TRATAMIENTOS QUE CONTIENEN DATOS DE NIVEL MEDIO O ALTO SÓLO DE FORMA ACCIDENTAL O ACCESORIA, PERO SIN GUARDAR RELACIÓN CON SU FINALIDAD. POR EJEMPLO, UN HOTEL DISPONE DE LOS DATOS DE ALERGIAS ALIMENTARIAS DE UN CLIENTE. ÉSTE ES UN DATO DE NIVEL ALTO POR REFERIRSE A LA SALUD, PERO ESTÁ EN EL FICHERO DE FORMA INCIDENTAL, PUES LA FINALIDAD DE DICHO FICHERO ES EL HOSPEDAJE.

4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS

NIVEL MEDIO

SON FICHEROS O TRATAMIENTOS DE NIVEL MEDIO, ENTRE OTROS, AQUELLOS RELATIVOS A LA PRESTACIÓN DE SERVICIOS DE SOLVENCIA PATRIMONIAL Y CRÉDITOS, AQUELLOS DE LOS QUE SEAN RESPONSABLES ENTIDADES FINANCIERAS PARA LAS FINALIDADES RELACIONADAS CON LA PRESTACIÓN DE SERVICIOS FINANCIEROS Y AQUELLOS QUE CONTENGAN UN CONJUNTO DE DATOS QUE OFREZCAN UNA DEFINICIÓN DE LAS CARACTERÍSTICAS O DE LA PERSONALIDAD Y QUE PERMITAN EVALUAR DETERMINADOS ASPECTOS DE LA PERSONALIDAD O DEL COMPORTAMIENTO DE LAS PERSONAS.

UNA DE LAS MEDIDAS QUE SE DEBE IMPLANTAR PARA ESTOS FICHEROS O TRATAMIENTOS DE DATOS DE NIVEL MEDIO ES LA REALIZACIÓN DE UNA AUDITORÍA (INTERNA O EXTERNA) CADA DOS AÑOS A FIN DE VERIFICAR QUE SE CUMPLEN LAS MEDIDAS DE SEGURIDAD QUE EXIGE LA NORMATIVA DE PROTECCIÓN DE DATOS.

4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS

NIVEL ALTO

SON FICHEROS O TRATAMIENTOS DE NIVEL ALTO, ENTRE OTROS, LOS QUE SE REFIEREN A DATOS DE IDEOLOGÍA, AFILIACIÓN SINDICAL, RELIGIÓN, CREENCIAS, ORIGEN RACIAL, SALUD O VIDA SEXUAL.

UNA DE LAS MEDIDAS DE SEGURIDAD QUE SE DEBE IMPLANTAR EN ESTOS FICHEROS DE NIVEL ALTO (SI SON AUTOMATIZADOS) ES, POR EJEMPLO, LA DEL REGISTRO DE ACCESOS, DE MANERA QUE QUEDE REGISTRADO EL USUARIO QUE HA INTENTADO ACCEDER AL FICHERO, LA HORA, EL FICHERO, EL TIPO DE ACCESO Y SI DICHO ACCESO HA SIDO AUTORIZADO O DENEGADO.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. **PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN**
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

EN EL MOMENTO DE DECIDIR LOS DISTINTOS PERFILES DE ACCESO QUE VA A DEFINIR LA ORGANIZACIÓN **HAY QUE TENER EN CUENTA LOS DISTINTOS ROLES FUNCIONALES** DE SU PERSONAL.

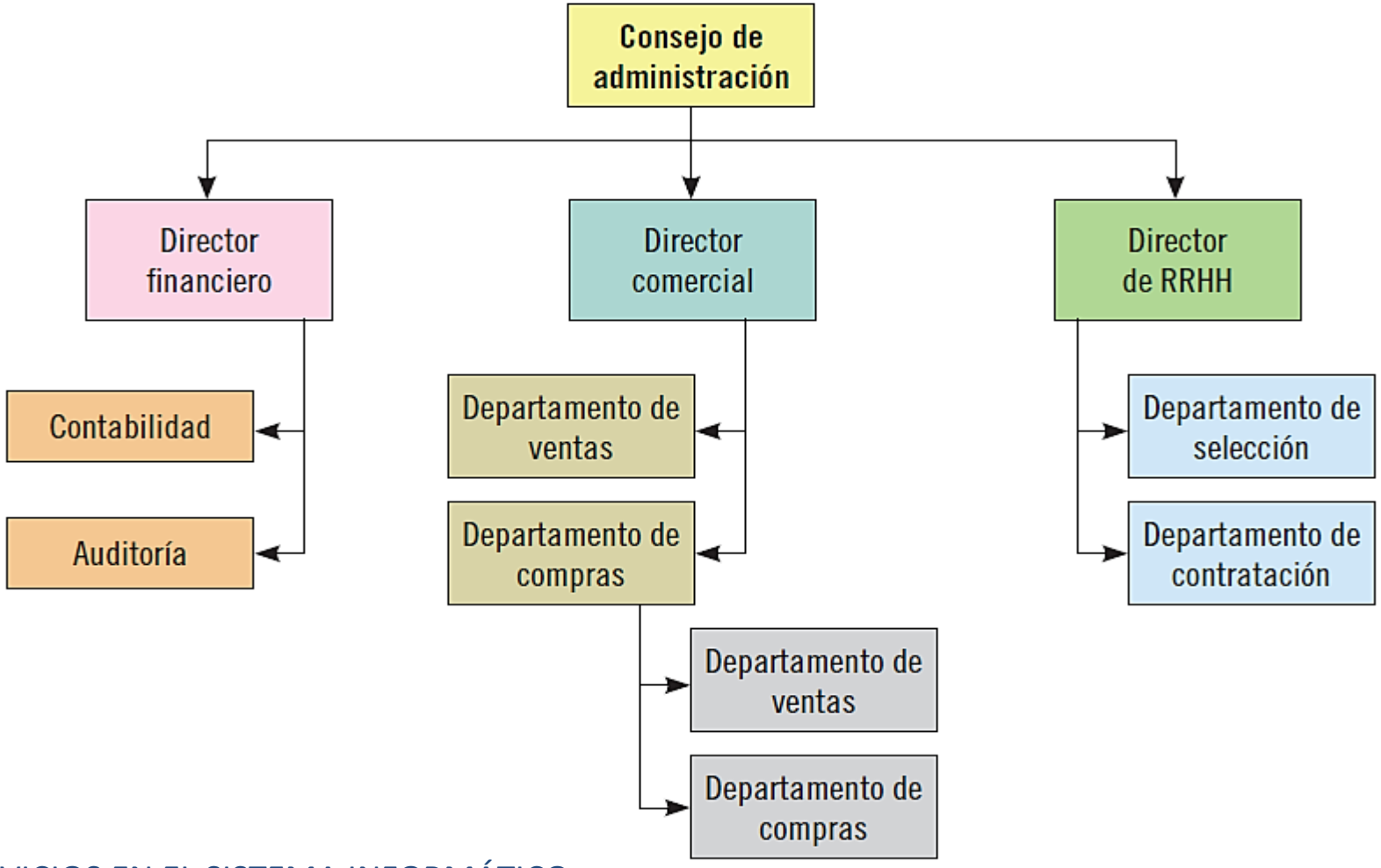
CUANDO SE QUIEREN DEFINIR LOS ROLES, ANTES DE NADA, HAY QUE VISUALIZAR Y TENER CLARO EL **ORGANIGRAMA DE LA ORGANIZACIÓN.**

UN ORGANIGRAMA NO ES MÁS QUE LA REPRESENTACIÓN GRÁFICA DE LA ESTRUCTURA DE UNA EMPRESA U ORGANIZACIÓN.

EN ÉL SE REPRESENTAN LOS DISTINTOS DEPARTAMENTOS QUE FORMAN PARTE DE LA ORGANIZACIÓN, SUS COMPETENCIAS Y LAS RELACIONES JERÁRQUICAS QUE HAY ESTABLECIDAS ENTRE LOS DISTINTOS PUESTOS Y DEPARTAMENTOS.

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

EJEMPLO DE ORGANIGRAMA



5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

UNA VEZ CLARA LA ESTRUCTURA FUNCIONAL DE LA ORGANIZACIÓN, HABRÍA QUE **DESCRIBIR LAS FUNCIONALIDADES Y RESPONSABILIDADES DE CADA PUESTO DE TRABAJO Y DECIDIR HASTA QUÉ NIVEL DE SEGURIDAD DEBEN PODER ACCEDER LOS EMPLEADOS PERTENECIENTES A CADA PUESTO**.

LUEGO, HABRÁ QUE CONCRETAR TODOS Y CADA UNO DE LOS EMPLEADOS QUE PERTENECEN A CADA PUESTO Y **OTORGAR PERMISOS, IDENTIFICADORES Y CONTRASEÑAS PERSONALIZADOS EN FUNCIÓN DE SU NIVEL DE RESPONSABILIDAD Y DEL NIVEL DE SEGURIDAD AL QUE PUEDEN ACCEDER,** PARA EL DESEMPEÑO CORRECTO DE SUS TAREAS DE TRABAJO.

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

TIPOS DE ACCESO

SOLO LECTURA

EL USUARIO CON ESTOS PERMISOS SOLO PODRÁ LEER Y VISUALIZAR LOS FICHEROS. NO PODRÁ EJECUTAR NINGUNA APLICACIÓN.

LISTA DE CONTENIDOS

EL USUARIO PODRÁ ABRIR LAS CARPETAS PARA VISUALIZAR LOS ARCHIVOS QUE HAY EN ELLA, PERO NO PODRÁ ACCEDER A ELLOS

LEER Y EJECUTAR

EL USUARIO PODRÁ EJECUTAR AQUELLAS APLICACIONES QUE NO INFLUYAN EN LOS DATOS DE LA ORGANIZACIÓN Y TAMBIÉN PODRÁ VISUALIZAR LOS ARCHIVOS, AUNQUE NO PODRÁ REALIZAR NINGUNA MODIFICACIÓN EN ELLOS

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

TIPOS DE ACCESO

LEER Y MODIFICAR

CON ESTOS PRIVILEGIOS, EL USUARIO, ADEMÁS DE PODER VISUALIZAR LOS ARCHIVOS, PODRÁ REALIZAR MODIFICACIONES EN LOS ARCHIVOS VISTOS. TAMBIÉN PODRÁ EJECUTAR APLICACIONES Y MODIFICAR ARCHIVOS A TRAVÉS DE ELLAS. NO OBSTANTE, NO TIENE PERMISO PARA CREAR ARCHIVOS NUEVOS NI ELIMINAR LOS EXISTENTES

CONTROL TOTAL

EL USUARIO YA ESTÁ AUTORIZADO PARA HACER CUALQUIER TIPO DE OPERACIÓN EN LOS ARCHIVOS SOBRE LOS QUE SE LES HA ASIGNADO ESTE PERMISO, DESDE SU CREACIÓN, MODIFICACIÓN HASTA SU ELIMINACIÓN

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

LA ASIGNACIÓN DE PERMISOS TIENE QUE SER COHERENTE CON LA JERARQUÍA ESTABLECIDA EN EL ORGANIGRAMA DE LA ORGANIZACIÓN:

- LOS USUARIOS CON MENORES RESPONSABILIDADES DEBERÁN TENER MENOS PRIVILEGIOS O SOLO SOBRE ARCHIVOS MENOS RELEVANTES.
- LOS ALTOS DIRECTIVOS DEBERÁN TENER PRIVILEGIOS PARA EJERCER EL CONTROL TOTAL DE LOS ARCHIVOS DE SU COMPETENCIA.

DE ESTE MODO, **LA ESTRUCTURA DE LOS PERMISOS** QUE SE VAN A OTORGAR A LOS USUARIOS **DEBE RESPONDER CON LA ESTRUCTURA REAL DE LA ORGANIZACIÓN**.

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

ADEMÁS, **LOS PERMISOS ASIGNADOS A CADA PUESTO DE TRABAJO SERÁN SOBRE LOS ARCHIVOS ESTRICTAMENTE NECESARIOS** PARA EL DESEMPEÑO EFECTIVO DE SU TRABAJO, NUNCA DANDO PERMISOS PARA VISUALIZAR O MODIFICAR ARCHIVOS QUE NO SON DE SU COMPETENCIA.

CON UNA CORRECTA ASIGNACIÓN DE PERMISOS ACORDE A LOS ROLES DEFINIDOS DENTRO DE UNA ORGANIZACIÓN YA **SE PODRÁ LLEVAR A CABO UN CONTROL DE SEGURIDAD ÓPTIMO SOBRE LOS ACCESOS A LOS ARCHIVOS DE LA ORGANIZACIÓN**.

5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN

ES RECOMENDABLE, Y EN OCASIONES OBLIGATORIO, QUE **LA ASIGNACIÓN DE PERMISOS DE ACCESO Y PRIVILEGIOS DEBE DOCUMENTARSE FORMALMENTE**, INFORMANDO A CADA EMPLEADO DE LOS PERMISOS QUE TIENE, DE SUS **DERECHOS Y OBLIGACIONES**, ADEMÁS DE LAS **SANCIONES** EN LAS QUE PUEDE INCURRIR EN CASO DE VIOLAR DICHOS PERMISOS.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. **HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL**
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

EL **DIRECTORIO ACTIVO** ES UN SERVICIO DE DIRECTORIO QUE **GESTIONA TODOS LOS ELEMENTOS QUE FORMAN PARTE DE UNA RED**, DESDE EQUIPOS HASTA GRUPOS, USUARIOS, DOMINIOS, POLÍTICAS DE SEGURIDAD Y CUALQUIER OTRO OBJETO QUE ESTÉ DEFINIDO POR EL USUARIO.

FUNCIONES DEL DIRECTORIO ACTIVO

LAS FUNCIONES DEL DIRECTORIO ACTIVO SE DEFINEN EN TORNO A TRES ÁREAS:

- **GESTIÓN DE IDENTIDAD**
- **SEGURIDAD**
- **GESTIÓN DE LA CONFIGURACIÓN**

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO

GESTIÓN DE IDENTIDAD

EL DIRECTORIO ACTIVO **SE ENCARGA DE IDENTIFICAR INEQUÍVOCAMENTE A CUALQUIER PERSONA** DE UNA ORGANIZACIÓN MEDIANTE:

- LA ELABORACIÓN Y REVISIÓN DE UN REPOSITORIO CENTRAL DE USUARIOS, SERVIDORES Y PUESTOS.
- LA REDUCCIÓN A LO ESENCIAL DEL NÚMERO DE REPOSITORIOS Y CONTRASEÑAS.
- EL ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD, VALIDACIÓN Y AUTORIZACIÓN.

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO

SEGURIDAD

EL DIRECTORIO ACTIVO TIENE COMO FUNCIÓN LA **ORGANIZACIÓN Y SIMPLIFICACIÓN DE LA LOCALIZACIÓN Y EL ACCESO A LOS DISTINTOS RECURSOS** DE LA RED DE LA ORGANIZACIÓN. ADEMÁS, TAMBIÉN **APLICA LAS POLÍTICAS DE SEGURIDAD ESTABLECIDAS EN LA ORGANIZACIÓN** MEDIANTE UNA HERRAMIENTA DE GESTIÓN UNIFICADA.

TODO ELLO, A TRAVÉS DE:

- LA AUTOMATIZACIÓN DEL BLOQUEO DE SISTEMAS OPERATIVOS
- EL REFUERZO DE LA UTILIZACIÓN DE CONTRASEÑAS Y CREDENCIALES
- LA POSIBILIDAD DE DELEGAR TAREAS ADMINISTRATIVAS PARA CONSEGUIR UNA ADMINISTRACIÓN HOMOGÉNEA

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO
GESTIÓN DE LA CONFIGURACIÓN

EL DIRECTORIO ACTIVO REALIZA UNA **GESTIÓN DE LA CONFIGURACIÓN DE LOS ELEMENTOS DE LA RED** PARA CONSEGUIR AUMENTAR LA PRODUCTIVIDAD DEL USUARIO Y REDUCIR LOS COSTES DE ADMINISTRACIÓN, SOPORTE Y APRENDIZAJE.

PARA CONSEGUIR ESTOS OBJETIVOS, **SE BASA EN FUNCIONES COMO**:

- LA GESTIÓN UNO A MUCHOS DE LOS USUARIOS Y EQUIPOS.
- LA AUTOMATIZACIÓN DEL FORZADO DE LAS POLÍTICAS DE SEGURIDAD.
- UNA IMPLEMENTACIÓN EFICIENTE DE LAS CONFIGURACIONES ESTÁNDAR PARA USUARIOS, GRUPOS DE USUARIOS Y EQUIPOS.

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO

EL DIRECTORIO ACTIVO ESTÁ CONSTRUIDO ALREDEDOR DE UNA SERIE DE PROTOCOLOS DE PLATAFORMA INDEPENDIENTE QUE PERMITEN TRABAJAR TANTO CON SISTEMAS OPERATIVOS **WINDOWS, LINUX O MACINTOSH**.

LOS PRINCIPALES PROTOCOLOS SON LOS SIGUIENTES:

- **LDAP**
- **DHCP**
- **DNS**
- **KERBEROS**

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO

LDAP

SE TRATA DE UN PROTOCOLO QUE **PERMITE EL ACCESO A UN SERVICIO DE DIRECTORIO ORDENADO Y DISTRIBUIDO CUYA FUNCIÓN PRINCIPAL ES PERMITIR LA BÚSQUEDA DE INFORMACIÓN EN UN ENTORNO DE RED**. EN NUMEROSAS OCASIONES, ES CONSIDERADO COMO UNA BASE DE DATOS SOBRE LA QUE SE PUEDEN REALIZAR UNA SERIE DE CONSULTAS PARA LOCALIZAR LOS DATOS DESEADOS.

DHCP

ES UN PROTOCOLO **QUE ASIGNA DE MODO AUTOMÁTICO LAS DIRECCIONES IP.**

6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL

FUNCIONES DEL DIRECTORIO ACTIVO

DNS

ES UNA BASE DE DATOS JERÁRQUICA EN LA QUE SE ALMACENA INFORMACIÓN SOBRE LOS NOMBRES DE DOMINIO EN LAS REDES. SU UTILIZACIÓN MÁS FRECUENTE SE RELACIONA CON LA ASIGNACIÓN DE NOMBRES DE DOMINIO A LAS DIRECCIONES IP.

KERBEROS

ES UN PROTOCOLO DE **AUTENTICACIÓN DE USUARIOS** QUE PERMITE QUE DOS EQUIPOS SITUADOS **EN UNA RED DE BAJA SEGURIDAD** SE PUEDAN IDENTIFICAR MUTUAMENTE **DE UN MODO SEGURO**.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. **HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)**
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

LA **IDENTIDAD** ***ES LA REPRESENTACIÓN DE UN INDIVIDUO O ENTIDAD DENTRO DE UN SISTEMA DE INFORMACIÓN***. ES LO QUE PERMITE DISTINGUIR A UN USUARIO DE LOS DEMÁS. UN PERFIL DE IDENTIDAD **INCLUYE ASPECTOS COMO**:

- IDENTIFICACIÓN ÚNICA.
- INFORMACIÓN PERSONAL DEL USUARIO.
- CREDENCIALES DE AUTENTICACIÓN.
- PERMISOS DE ACCESO Y ROLES ASIGNADOS AL USUARIO.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

LA GESTIÓN DE IDENTIDADES Y AUTORIZACIONES **(IAM) ES UN CONJUNTO DE SISTEMAS Y PROCESOS ENCARGADOS DE GESTIONAR Y CONTROLAR LA IDENTIDAD DE LAS PERSONAS QUE ACCEDEN A LOS RECURSOS DEL SISTEMA DE INFORMACIÓN Y TODO AQUELLO QUE PUEDE HACER CADA USUARIO CON ESTOS RECURSOS**, CUMPLIENDO EN TODO MOMENTO CON LAS POLÍTICAS DEFINIDAS POR LA ORGANIZACIÓN.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

LA GESTIÓN DE IDENTIDADES APORTA **FUNCIONALIDADES** COMO:

- **CREACIÓN Y MANTENIMIENTO DE PERFILES**
  LO QUE SIMPLIFICA LA GESTIÓN DE LOS USUARIOS.
- **FACILITA O DENIEGA EL ACCESO A LOS RECURSOS**
  TANTO LÓGICOS COMO FÍSICOS, A LOS USUARIOS ADECUADOS.
- **AÑADE VISIBILIDAD A LOS SERVICIOS DE LA ORGANIZACIÓN**
  AMPLIANDO DE UN MODO SEGURO LOS SERVICIOS QUE ESTA OFRECE A LOS USUARIOS.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

LAS HERRAMIENTAS **IAM** SE UTILIZAN SOBRE TODO PARA *ADMINISTRAR LA AUTENTICACIÓN DE LOS USUARIOS, LOS DERECHOS Y RESTRICCIONES DE ACCESO, LOS DISTINTOS PERFILES DE CUENTAS, CONTRASEÑAS* Y OTROS CONCEPTOS BÁSICOS PARA ADMINISTRAR LOS PERFILES DE ACCESO A UNA APLICACIÓN.

CON LAS HERRAMIENTAS IAM SE PUEDEN LLEVAR A CABO ACCIONES COMO:

- **PROVISIÓN O DESPROVISIÓN DE CUENTAS**
- **AUTOMATIZACIÓN DEL FLUJO DE TRABAJO**
- **ADMINISTRACIÓN REMOTA**
- **SINCRONIZACIÓN DE CONTRASEÑAS**
- **REEMPLAZO AUTOMÁTICO DE CONTRASEÑAS**

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

PROVISIÓN O DESPROVISIÓN DE CUENTAS

DAR DE ALTA CUENTAS NUEVAS EN EL MOMENTO QUE UN NUEVO USUARIO DEBE PODER ACCEDER AL SISTEMA Y DAR DE BAJA LAS CUENTAS CUANDO EL USUARIO QUE LAS UTILIZABA YA NO DEBE ACCEDER AL MISMO.

AUTOMATIZACIÓN DEL FLUJO DE TRABAJO

LAS HERRAMIENTAS **IAM** PERMITEN AUTOMATIZAR TAREAS QUE FACILITAN LA INTEGRACIÓN DE LOS DISTINTOS PROCESOS DE AUTENTICACIÓN Y AUTORIZACIÓN DE LOS USUARIOS DE LA ORGANIZACIÓN.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

ADMINISTRACIÓN REMOTA

CON LAS HERRAMIENTAS **IAM** SE PUEDEN GESTIONAR LAS IDENTIDADES DESDE EQUIPOS EXTERNOS CON UNA SIMPLE CONEXIÓN A INTERNET.

SINCRONIZACIÓN DE CONTRASEÑAS

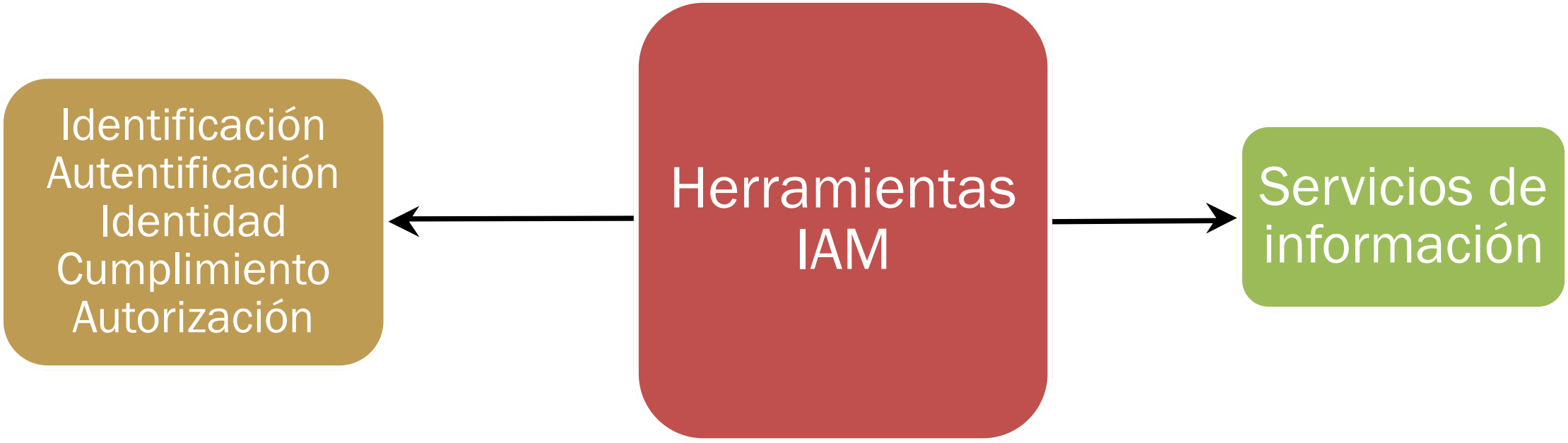
CON LAS HERRAMIENTAS **IAM** SE PUEDEN GESTIONAR LAS IDENTIDADES DESDE EQUIPOS EXTERNOS CON UNA SIMPLE CONEXIÓN A INTERNET.

REEMPLAZO AUTOMÁTICO DE CONTRASEÑAS

EN EL MOMENTO QUE HAY VARIOS INTENTOS DE ACCESO NO AUTORIZADOS, LAS HERRAMIENTAS DE GESTIÓN DE IDENTIDADES PERMITEN EL REEMPLAZO AUTOMÁTICO DE LAS CONTRASEÑAS PARA IMPEDIR ESTE TIPO DE ACCESO.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

LA GESTIÓN DE IDENTIDADES ES EL PUENTE ENTRE LAS PERSONAS FÍSICAS Y LOS RECURSOS QUE *FACILITAN LOS SERVICIOS DE INFORMACIÓN EN CUANTO A IDENTIFICACIÓN, AUTENTIFICACIÓN, IDENTIDAD Y AUTORIZACIÓN DE USUARIOS Y A CUMPLIMIENTO DE LA POLÍTICA DE LA ORGANIZACIÓN*.



7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

COMO **VENTAJAS** PRINCIPALES DE ESTAS HERRAMIENTAS DESTACAN:

- LA MEJORA DE LA SEGURIDAD DE LA ORGANIZACIÓN,
- LA CONSOLIDACIÓN DE LAS POLÍTICAS DE SEGURIDAD DEFINIDAS
- LA REDUCCIÓN DE LOS COSTES DE ADMINISTRACIÓN.

ESTAS HERRAMIENTAS **IAM** SON SOLUCIONES MUY ADECUADAS ANTE UN ENTORNO DONDE EL DESARROLLO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN ES CRECIENTE Y MÁS CONCRETAMENTE PORQUE **PROPORCIONAN SOLUCIONES** A LAS PROBLEMÁTICAS SIGUIENTES:

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

- CADA VEZ HAY UN MAYOR NÚMERO DE USUARIOS, TANTO INTERNOS COMO EXTERNOS QUE DEBEN ACCEDER A LOS RECURSOS DEL SISTEMA DE INFORMACIÓN DE LA ORGANIZACIÓN.
- HAY UN NÚMERO CRECIENTE DE OPORTUNIDADES DE NEGOCIO A TRAVÉS DEL DESARROLLO DE LAS NUEVAS TECNOLOGÍAS, QUE REQUIERE UN MAYOR NIVEL DE CONTROL Y SEGURIDAD EN LAS OPERACIONES DE LA ORGANIZACIÓN.
- HAY NUMEROSAS APLICACIONES Y SISTEMAS QUE CUENTAN CON SUS PROPIAS FORMAS DE AUTENTICACIÓN Y AUTORIZACIÓN.
- LOS USUARIOS DISPONEN DE MÚLTIPLES AUTORIZACIONES QUE SE BASAN EN DISTINTOS MECANISMOS DE AUTORIZACIÓN Y ES NECESARIO UN SISTEMA INTEGRADOR.
- LOS REQUERIMIENTOS LEGALES EXIGEN CONTROLES MUY ELEVADOS DE SEGURIDAD.
- EL AUMENTO DE COMPETENCIA EN LOS MERCADOS EXIGE UNA REDUCCIÓN DE LOS COSTES, QUE LAS HERRAMIENTAS AIM SON CAPACES DE FACILITAR.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

TAMBIÉN HAY QUE TENER EN CUENTA UNA SERIE DE **DESVENTAJAS**:

- LA FUNCIONALIDAD DE SINCRONIZACIÓN DE CONTRASEÑAS SUPONE UN INCREMENTO DE LOS RIESGOS DE SEGURIDAD, YA QUE SI SE DESCUBRE UNA CONTRASEÑA SE PUEDE ACCEDER A TODAS LAS APLICACIONES A LAS QUE EL USUARIO TIENE ACCESO.
- EN LAS HERRAMIENTAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES, EL ACCESO A LAS APLICACIONES SE REALIZA MEDIANTE LA AUTENTICACIÓN DE LOS USUARIOS. SI HAY ALGÚN FALLO EN LOS PROCESOS DE AUTENTICACIÓN Y AUTORIZACIÓN, ESTO AFECTARÍA A TODAS LAS APLICACIONES INTEGRADAS EN ESTAS HERRAMIENTAS.
- LA IMPLEMENTACIÓN DE ESTAS HERRAMIENTAS SUELE REQUERIR UNA REESTRUCTURACIÓN DE LOS PROCESOS Y DE LA OPERATIVA DE LAS ORGANIZACIONES, LO QUE SUPONE TIEMPO, GASTO Y RECURSOS.
- LA IMPLEMENTACIÓN DE ESTAS HERRAMIENTAS REQUIERE UNA ELEVADA INVERSIÓN DE DINERO, TIEMPO Y RECURSOS, LO QUE NO RESULTARÍA VIABLE PARA PROYECTOS A CORTO PLAZO.
- ES NECESARIO TENER UN CONOCIMIENTO PROFUNDO DE LAS APLICACIONES QUE SE PRETENDEN INTEGRAR EN LA SOLUCIÓN **IAM** PARA QUE LAS CONFIGURACIONES DE AUTENTICACIÓN Y AUTORIZACIÓN SE REALICEN CORRECTAMENTE.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

A CONTINUACIÓN, SE MUESTRAN ALGUNAS HERRAMIENTAS **IAM**:

- **SOLARWINDS ACCESS RIGHTS MANAGER**
- **MICROSOFT AZURE ACTIVE DIRECTORY**
- **SERVICIO ORACLE IDENTITY CLOUD**
- **IBM SECURITY IDENTITY AND ACCESS ASSURANCE**
- **SAILPOINT IDENTITYIQ**

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

SOLARWINDS ACCESS RIGHTS MANAGER

UNA INTERFAZ QUE TAMBIÉN PROPORCIONA FUNCIONES DE SEGURIDAD, COMO PREVENCIÓN DE PÉRDIDA DE DATOS Y BÚSQUEDA DE AMENAZAS. ESTA HERRAMIENTA TAMBIÉN PROPORCIONA HERRAMIENTAS DE REGISTRO Y AUDITORÍA PARA EL CUMPLIMIENTO DE LOS ESTÁNDARES DE DATOS.

ESTE PAQUETE NO SOLO ADMINISTRA LOS DERECHOS DE ACCESO, TAMBIÉN CLASIFICA LA SENSIBILIDAD DE LOS RECURSOS, AUDITA EL ACCESO A LOS RECURSOS E IDENTIFICA LAS CUENTAS VULNERABLES. ES UN SISTEMA DE PREVENCIÓN DE PÉRDIDA DE DATOS Y UNA HERRAMIENTA DE AUDITORÍA DE CUMPLIMIENTO DE DATOS, ASÍ COMO UN SISTEMA DE GESTIÓN DE DERECHOS DE ACCESO.

SOLARWINDS ACCESS RIGHTS MANAGER ES ADECUADO PARA EMPRESAS QUE NECESITAN DEMOSTRAR EL CUMPLIMIENTO DE LOS ESTÁNDARES DE SEGURIDAD DE DATOS.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

MICROSOFT AZURE ACTIVE DIRECTORY

ES LA SOLUCIÓN INTEGRAL DE GESTIÓN DE IDENTIDADES BASADA EN LA NUBE DE MICROSOFT. PUEDE ADMINISTRAR LOS DERECHOS DE ACCESO DE MILES DE CUENTAS DE INICIO DE SESIÓN CON FACILIDAD. TAMBIÉN PERMITE UNA CREDENCIAL DE AUTORIZACIÓN QUE PERMITE A TODOS LOS MIEMBROS DE UNA ORGANIZACIÓN ACCEDER Y LANZAR SUS APLICACIONES EN LA NUBE, SIN NINGUNA RESTRICCIÓN DEL SISTEMA OPERATIVO DE SU ELECCIÓN.

DEBIDO A QUE ES UN PRODUCTO DE MICROSOFT, **AZURE AD SE INTEGRA SIN PROBLEMAS CON EL DOMINIO DE AD LOCAL EXISTENTE Y CUALQUIER APLICACIÓN QUE SE EJECUTE EN LA NUBE Y LOS USUARIOS REMOTOS QUE SE CONECTAN A TRAVÉS DE INTERNET**.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

SERVICIO ORACLE IDENTITY CLOUD

ES UN IAM QUE FORMA PARTE DE ORACLE PUBLIC CLOUD (OPC). ES SU SERVICIO GRATUITO EN LA NUBE QUE SATISFACE LAS NECESIDADES DE LAS EMPRESAS QUE VAN DESDE EL ALMACENAMIENTO DE DATOS Y LOS SERVICIOS DE RED HASTA EL ESPACIO DE PRUEBA DE APLICACIONES Y MUCHO MÁS.

ES UN SERVICIO IAM ALTAMENTE ESCALABLE PORQUE SE BASA EN MICROSERVICIOS QUE EJECUTAN SUS PROPIOS PROCESOS CUANDO SE CONECTAN A ACTIVOS O MIENTRAS TRABAJAN CON DATOS. ESTO LO CONVIERTE EN UNA OPCIÓN IDEAL PARA EMPRESAS QUE SIEMPRE SE ESTÁN TRANSFORMANDO O CRECIENDO.

ESTA PLATAFORMA DE IAM **OFRECE ESCALABILIDAD INNOVADORA CON UN CONJUNTO DE PLATAFORMAS, APLICACIONES Y SERVICIOS LÍDERES EN LA INDUSTRIA, INCLUIDAS SOLUCIONES DE ADMINISTRACIÓN DE IDENTIDAD**.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

IBM SECURITY IDENTITY AND ACCESS ASSURANCE

ES UN IAM “SILENCIOSO” QUE FUNCIONA EN SINCRONÍA CON LOS PROCESOS Y OPERACIONES DE UNA ORGANIZACIÓN PARA QUE LOS USUARIOS DE LA RED NI SIQUIERA NOTEN QUE SE ESTÁ EJECUTANDO EN SEGUNDO PLANO.

UNA CARACTERÍSTICA QUE SE DESTACA DE ESTE IAM ES SU CAPACIDAD PARA PROTEGER CUENTAS PRIVILEGIADAS. PERMITE LA PROTECCIÓN Y ADMINISTRACIÓN DE CUENTAS PRIVILEGIADAS EN UNA ORGANIZACIÓN CON SEGURIDAD DE CONTRASEÑA DE NIVEL EMPRESARIAL Y ADMINISTRACIÓN DE ACCESO PRIVILEGIADO.

TAMBIÉN DESCUBRE, PROTEGE Y ADMINISTRA LAS CONTRASEÑAS DE ESTAS «SUPER» CUENTAS PARA PROTEGERLAS DEL ABUSO Y EL USO INDEBIDO.

PARA LAS ORGANIZACIONES QUE DESEAN LLEVAR SU SEGURIDAD AL SIGUIENTE NIVEL, ESTE IAM TAMBIÉN OFRECE AUTENTICACIÓN SIN CONTRASEÑA AL ADMITIR MÉTODOS DE INICIO DE SESIÓN COMO EL USO DE BIOMETRÍA, FACE ID, TOUCH ID, CORREO ELECTRÓNICO O CONTRASEÑAS DE UN SOLO USO POR SMS Y TOKENS DE SOFTWARE.

7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)

HERRAMIENTAS PARA GESTIÓN DE IDENTIDADES

SAILPOINT IDENTITYIQ

ESTÁ BIEN CONSIDERADO POR SU SÓLIDA GESTIÓN DE IDENTIDADES Y SUS CAPACIDADES DE APROVISIONAMIENTO. SE PUEDE UTILIZAR COMO UNA INSTALACIÓN LOCAL INDEPENDIENTE O COMO UNA SOLUCIÓN DE IDENTIDAD COMO SERVICIO (IDAAS).

LA OPCIÓN IDAAS SERÍA LA MEJOR OPCIÓN PARA LAS ORGANIZACIONES QUE PREFIEREN QUE SU IAM SEA MANEJADO POR PROFESIONALES SIN CONTRATAR EXPERTOS EN CIBERSEGURIDAD PROPIOS.

EL RENDIMIENTO DE ESTE IAM SE PUEDE MEJORAR AÚN MÁS INTEGRÁNDOLO CON LA IDENTIDAD PREDICTIVA DE SAILPOINT, SU IA Y PLATAFORMA BASADA EN LA NUBE IMPULSADA POR MÁQUINAS QUE RECOMIENDA QUÉ ACCESOS APROBAR O REVOCAR PARA UNA CUENTA SEGÚN LOS ATRIBUTOS Y PATRONES DE ACCESO.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. **HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)**

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

EL **INICIO DE SESIÓN ÚNICO, INICIO DE SESIÓN UNIFICADO O PUNTO ÚNICO DE AUTENTICACIÓN (SSO)** ES UN SISTEMA DE AUTENTICACIÓN DE SESIÓN ÚNICO QUE PERMITE AL USUARIO ACCEDER A MÚLTIPLES RECURSOS Y APLICACIONES A TRAVÉS DE UN ÚNICO LOGIN.

PERMITE ACCEDER A MÁS DE UN SERVICIO COMPLETANDO UNA ÚNICA VEZ TODOS LOS DATOS PERSONALES.

SSO PERMITE AL USUARIO IDENTIFICARSE UNA SOLA VEZ Y MANTENER LA SESIÓN ABIERTA PARA EL RESTO DE LAS APLICACIONES.

EL **SSO** ES UN SISTEMA IMPORTANTE PARA **LA GESTIÓN DE IDENTIDAD** Y **CONTROL DE ACCESO**.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

A CONTINUACIÓN, SE MUESTRAN ALGUNOS TIPOS DE **SSO**:

- **SAML 2.0**
- **OAUTH2**
- **CAS**
- **SHIBBOLETH**
- **TARJETA INTELIGENTE**
- **SSO PERSONALIZADO**

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

SAML 2.0

SAML 2.0 (SECURITY ACCESS MARKUP LANGUAGE) ES EL TIPO DE SSO MÁS COMÚN. ES UNA FORMA DE CODIFICAR TEXTO QUE SE USA ESPECÍFICAMENTE PARA INTERCAMBIAR INFORMACIÓN DE IDENTIFICACIÓN. TIENE UN ESTÁNDAR ABIERTO, POR LO QUE CUALQUIER PERSONA PUEDE TENER ACCESO A LA DOCUMENTACIÓN Y ES CONTRARIO AL ESTÁNDAR DE PROPIETARIO O ESTÁNDAR CERRADO, EL CUAL PERTENECE A UNA DETERMINADA EMPRESA Y NADIE MÁS PUEDE TENER PERMISO PARA UTILIZARLO.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

OAUTH2

TIENE UN PROCESO SIMILAR AL SAML 2.0, PERO CON CIERTAS DIFERENCIAS. LA MÁS NOTABLE ES SU OPTIMIZACIÓN; MIENTRAS QUE SAML ESTÁ ESPECIALIZADO PARA APLICACIONES WEB, OAUTH ES MÁS ADECUADO PARA APLICACIONES NATIVAS; POR EJEMPLO, LA DE LOS TELÉFONOS INTELIGENTES.

MÁS ALLÁ DE ESTO SON IGUALES: DOS ESTÁNDARES PARA TRANSFERIR INFORMACIÓN DE IDENTIFICACIÓN QUE CIFRAN Y CONVIERTEN LOS DATOS INTRODUCIDOS EN UN CÓDIGO LEGIBLE SOLO POR MÁQUINA.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

CAS

EL SERVICIO DE AUTENTICACIÓN CENTRAL O CAS SE DIFERENCIA DEL SAML 2.0 AL PROMULGAR LA COMUNICACIÓN DE SERVIDOR A SERVIDOR. MIENTRAS QUE LA MÁQUINA DEL CLIENTE SE UTILIZA PARA INICIAR LA SOLICITUD DE TOKEN, LA VERIFICACIÓN FINAL ES GESTIONADA MEDIANTE UNA COMUNICACIÓN DE FONDO ENTRE EL SERVIDOR CAS Y EL PROVEEDOR DE SERVICIOS.

ESTE TIPO DE SSO LO USAN COMÚNMENTE ORGANIZACIONES EDUCATIVAS DEBIDO A LA DEPENDENCIA DE ESA VERIFICACIÓN ADICIONAL Y MÁS DIRECTA.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

SHIBBOLETH

ESTE TIPO DE PROTOCOLO SSO TAMBIÉN LO UTILIZAN LAS ENTIDADES EDUCATIVAS, ESPECÍFICAMENTE CUANDO UN GRAN NÚMERO DE INSTITUCIONES ESTÁN FEDERADAS PARA COMPARTIR APLICACIONES O SERVICIOS. SI BIEN SHIBBOLETH SE CREÓ CON SAML COMO BASE, USA DISCOVERY SERVICE PARA MEJORAR SU ORGANIZACIÓN DE DATOS EN UNA GRAN CANTIDAD DE FUENTES.

ESTE TIPO DE SSO AYUDA A AUTOMATIZAR EL ANÁLISIS DE METADATOS PARA MANEJAR ACTUALIZACIONES DE CERTIFICADOS DE SEGURIDAD Y OTRAS CONFIGURACIONES ESTABLECIDAS POR INSTITUCIONES INDIVIDUALES.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

TARJETA INTELIGENTE

LAS TARJETAS INTELIGENTES BASADAS EN SSO LE PIDEN AL USUARIO FINAL UTILIZAR UNA TARJETA CON LAS CREDENCIALES DE INICIO DE SESIÓN PARA EL PRIMER ACCESO. UNA VEZ HECHO ESTO, EL USUARIO NO TENDRÁ QUE VOLVER A INGRESAR NOMBRES DE USUARIO O CONTRASEÑAS. ESTAS TARJETAS SON CAPACES DE ALMACENAR CERTIFICADOS O CONTRASEÑAS.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

TIPOS SSO

SSO PERSONALIZADO

SE DEBE CONFIGURAR UN SERVIDOR DE AUTORIZACIÓN, ESTABLECER UN ESTÁNDAR PARA COMUNICAR INFORMACIÓN DE IDENTIFICACIÓN, ASEGURARTE DE QUE TODO SEA SEGURO Y GARANTIZAR QUE TODAS LAS APLICACIONES UTILIZADAS POR TU EMPRESA PUEDAN COMUNICARSE BAJO ESE ESTÁNDAR.

SUENA COMPLICADO PORQUE LO ES. POR ELLO, EXISTEN MÁS TIPOS DE SSO MENOS COMPLEJOS Y MÁS FÁCILES DE IMPLEMENTAR, PERO SI ES LA OPCIÓN QUE MÁS VENTAJAS TE OFRECE Y TIENES LOS RECURSOS NECESARIOS, PUEDES UTILIZARLA.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

A CONTINUACIÓN, SE MUESTRAN ALGUNAS HERRAMIENTAS **SSO**:

- **DUO + CISCO**
- **KEEPER**
- **LASTPASS**
- **RIPPLING**
- **OKTA**

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

DUO + CISCO

DUO CUENTA CON TODAS LAS FUNCIONES DE SSO Y ESTÁ BASADO EN UNA APLICACIÓN PARA SMARTPHONE EQUIVALENTE A LAS APLICACIONES DE GESTIÓN MÓVIL. SOPORTA DIVERSOS MÉTODOS DE AUTENTICACIÓN ADAPTATIVA.

CON ESTE SOFTWARE PUEDES PROTEGER TUS APLICACIONES Y DATOS A ESCALA BAJO UN MODELO DE SEGURIDAD ZERO TRUST, QUE VERIFICA LA IDENTIDAD DEL USUARIO Y ESTADO DEL DISPOSITIVO EN CADA INTENTO DE INICIO DE SESIÓN.

SUS PRINCIPALES OBJETIVOS SON GENERAR CONFIANZA EN EL USUARIO Y DISPOSITIVO, OBTENER VISIBILIDAD DE DISPOSITIVOS Y HABILITAR EL ACCESO SEGURO A TODAS LAS APLICACIONES.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

KEEPER

ES UN GESTOR DE CONTRASEÑAS Y BÓVEDA DIGITAL QUE UTILIZA CIFRADO DEL TIPO AES DE 265 BITS Y PBKDF2.

SU PRINCIPAL FUNCIÓN ES REDUCIR EL RIESGO DE INFRACCIONES DE DATOS.

PUEDE SER UTILIZADO EN NAVEGADORES WEB, EQUIPOS INFORMÁTICOS Y DISPOSITIVOS MÓVILES.

ENTRE SUS PRINCIPALES FUNCIONES SE ENCUENTRAN LA CREACIÓN DE CONTRASEÑAS ALEATORIAS DE ALTA SEGURIDAD PARA USUARIOS Y LA GESTIÓN DE ACCESO DE USUARIO A DATOS CONFIDENCIALES.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

LASTPASS

BRINDA UNA UBICACIÓN CENTRAL DESDE LA CUAL LOS USUARIOS PUEDEN ADMINISTRAR TODOS LOS INICIOS DE SESIÓN Y CONTRASEÑAS DE LOS COLABORADORES QUE CONFORMAN UNA EMPRESA.

PUEDE USARSE EN MÚLTIPLES DISPOSITIVOS Y SU EDICIÓN EMPRESARIAL PROPORCIONA GESTIÓN SEGURA DE CONTRASEÑAS PARA EMPRESAS, YA QUE OFRECE MÁS DE 50 POLÍTICAS INTEGRADAS Y CONFIGURABLES PARA ESTABLECER REQUISITOS DE CONTRASEÑA MAESTRA, RESTRINGIR ACCESO A DISPOSITIVOS Y UBICACIONES ESPECÍFICAS.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

RIPPLING

ES UN TIPO DE SISTEMA SSO ESPECÍFICO PARA EL ÁREA DE RECURSOS HUMANOS Y TI CON EL QUE PUEDEN GESTIONAR LAS ALTAS Y PROCESOS DE CADA EMPLEADO.

TODO SE REALIZA EN UNA MISMA PLATAFORMA VERSÁTIL Y FÁCIL DE USAR.

SU FUNCIÓN PRINCIPAL ES CONFIGURAR O DESACTIVAR EL ALTA DE UN EMPLEADO A LA NÓMINA, SU SEGURO DE SALUD, DAR ACCESO A LA COMPUTADORA EMPRESARIAL Y APLICACIONES COMO GMAIL O SLACK Y AUTOMATIZAR TODO EL TRABAJO ADMINISTRATIVO.

8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

HERRAMIENTAS SSO

OKTA

CUENTA CON DOS VERSIONES ADAPTABLES QUE SIRVEN PARA DETECTAR LA UBICACIÓN, DISPOSITIVOS Y PARÁMETROS DE RED PARA EVITAR ATAQUES DE FALSIFICACIÓN.

EN SUS ÚLTIMAS ACTUALIZACIONES INCLUYERON EL SERVICIO DE GESTIÓN DEL CICLO DE VIDA PARA OFFICE 365, INTEGRACIÓN DE DIRECTORIOS CON AD O LDAP Y APROVISIONAMIENTO AUTOMÁTICO.

CONTENIDOS

1. INTRODUCCIÓN
2. ANÁLISIS DE LOS REQUERIMIENTOS DE ACCESO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN Y RECURSOS COMPARTIDOS
3. PRINCIPIOS COMÚNMENTE ACEPTADOS PARA EL CONTROL DE ACCESOS Y DE LOS DISTINTOS TIPOS DE ACCESO LOCALES Y REMOTOS
4. REQUERIMIENTOS LEGALES EN REFERENCIA AL CONTROL DE ACCESOS Y ASIGNACIÓN DE PRIVILEGIOS
5. PERFILES DE ACCESO EN RELACIÓN CON LOS ROLES FUNCIONALES DEL PERSONAL DE LA ORGANIZACIÓN
6. HERRAMIENTAS DE DIRECTORIO ACTIVO Y SERVIDORES LDAP EN GENERAL
7. HERRAMIENTAS DE SISTEMAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES (IAM)
8. HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN: SINGLE SIGN ON (SSO)

RESUMEN

ES FUNDAMENTAL **REALIZAR UN ANÁLISIS INICIAL DE LOS REQUERIMIENTOS DE ACCESO** EN EL MOMENTO DE **DEFINIR LA POLÍTICA DE ACCESO DE LOS SISTEMAS DE INFORMACIÓN** DE UNA ORGANIZACIÓN.

ESTOS REQUERIMIENTOS SE ENCUENTRAN RECOGIDOS PRINCIPALMENTE EN LA NORMATIVA **ISO/IEC 27002** Y, CONCRETAMENTE, EN EL APARTADO **9**.

ADEMÁS DE LA NORMATIVA MENCIONADA, TAMBIÉN HAY QUE REFERIRSE AL **REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS UE 679/2016**, QUE HACE MENCIÓN A LAS MEDIDAS QUE DEBEN TOMAR LAS ORGANIZACIONES DEPENDIENDO DEL NIVEL DE SEGURIDAD DE LOS DATOS: **BÁSICO, MEDIO O ALTO**. A MAYOR NIVEL DE SEGURIDAD, MAYORES DEBEN SER LAS MEDIDAS A TOMAR.

RESUMEN

UNA VEZ DEFINIDA LA POLÍTICA DE SEGURIDAD DE LA EMPRESA Y REVISADAS LAS MEDIDAS DE SEGURIDAD QUE HAY QUE TOMAR, ATENDIENDO A LOS REQUERIMIENTOS LEGALES ESTABLECIDOS, YA SE PUEDEN **DEFINIR LOS DISTINTOS PERFILES DE ACCESO DE LA ORGANIZACIÓN** ATENDIENDO AL PUESTO DE TRABAJO QUE OCUPAN DENTRO DE ELLA.

NO TODOS LOS EMPLEADOS DEBEN PODER ACCEDER Y UTILIZAR EL MISMO TIPO DE INFORMACIÓN, TODO LO CONTRARIO: SERÁ VITAL OBSERVAR EL **ORGANIGRAMA DE LA ORGANIZACIÓN Y LAS FUNCIONALIDADES Y RESPONSABILIDADES** DE CADA PUESTO DE TRABAJO PARA ASÍ ASIGNARLES ACCESO Y PRIVILEGIOS EXCLUSIVAMENTE A LA INFORMACIÓN NECESARIA Y PERTINENTE PARA CADA EMPLEADO.

RESUMEN

HAY VARIAS HERRAMIENTAS DE CONTROL DE ACCESOS:

- LAS **HERRAMIENTAS DE DIRECTORIO ACTIVO** GESTIONAN TODOS LOS ELEMENTOS QUE FORMAN PARTE DE UNA RED
- **LAS HERRAMIENTAS DE GESTIÓN DE IDENTIDADES Y AUTORIZACIONES** (**IAM**) GESTIONAN LA IDENTIDAD DE LAS PERSONAS QUE ACCEDEN A LOS RECURSOS DEL SISTEMA DE INFORMACIÓN Y QUE PUEDE HACER CADA USUARIO CON ESTOS.
- LAS **HERRAMIENTAS DE SISTEMAS DE PUNTO ÚNICO DE AUTENTICACIÓN O SINGLE SIGN ON (SSO)**, QUE FACILITAN QUE LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN SOLO TENGAN QUE IDENTIFICARSE UNA VEZ PARA ACCEDER A LOS DISTINTOS SERVICIOS DEL SISTEMA DE INFORMACIÓN.

CON TODAS ESTAS HERRAMIENTAS, LAS ORGANIZACIONES PUEDEN LLEVAR A CABO **UNA POLÍTICA DE CONTROL DE ACCESOS ACTIVA Y EFICIENTE Y AUMENTAR ASÍ EL NIVEL DE SEGURIDAD DE LA ORGANIZACIÓN**.

ESTO ES TODO