TECNOLOGÍA ANÁLISIS Y DESARROLLO DE SOFTWARE

GA4-220501095-AA1-EV02

Modelos conceptual y lógico para el proyecto desarrollo de software

Ficha: 3134547

Instructora: Astrid Fernández

Cindy Tatiana Ballesteros Valbuena

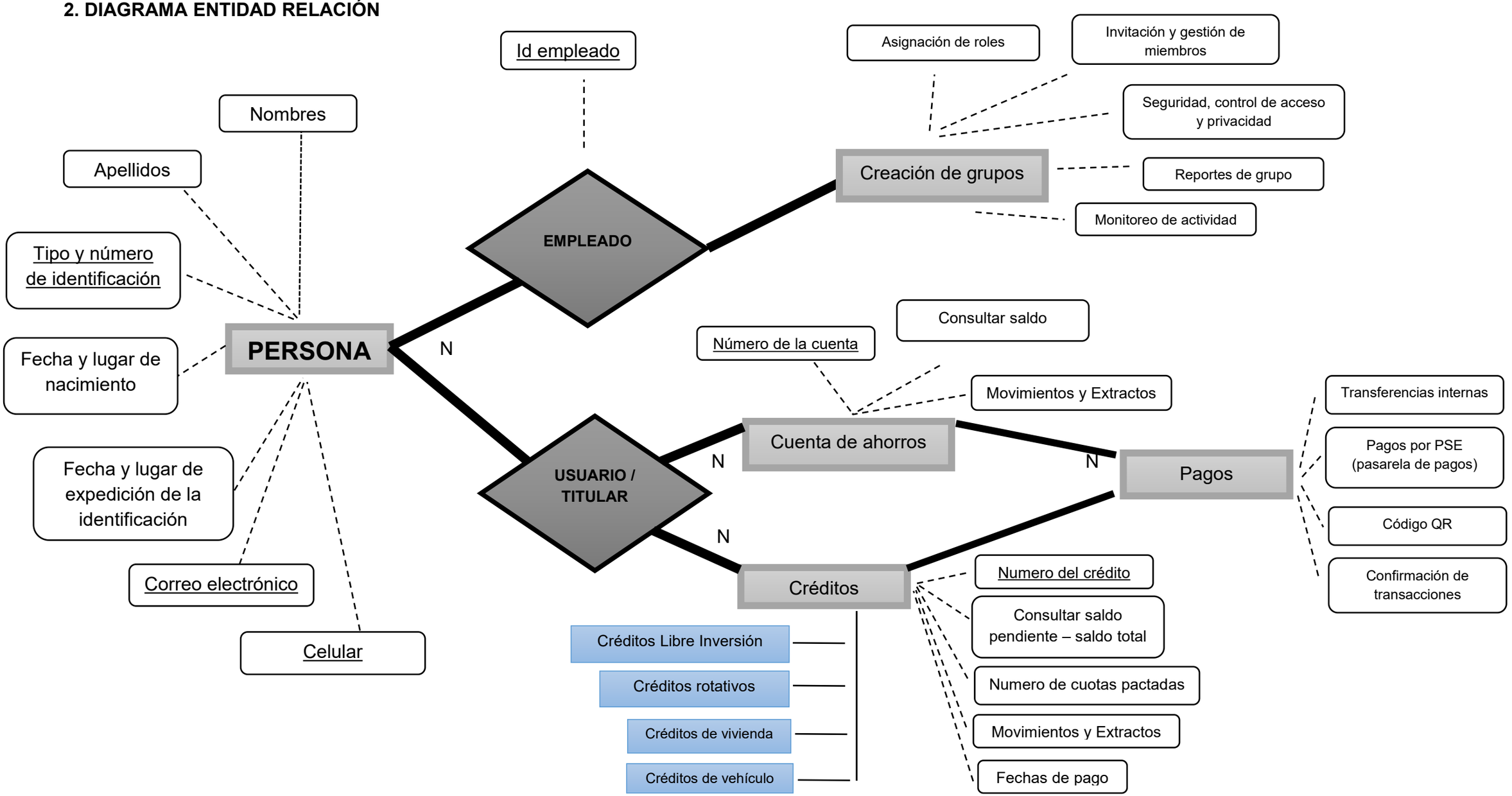
SERVICIO NACIONAL DE APRENDIZAJE – SENA
CENTRO DE COMERCIO Y SERVICIO REGIONAL
CAUCA
2025

TABLA DE CONTENIDO

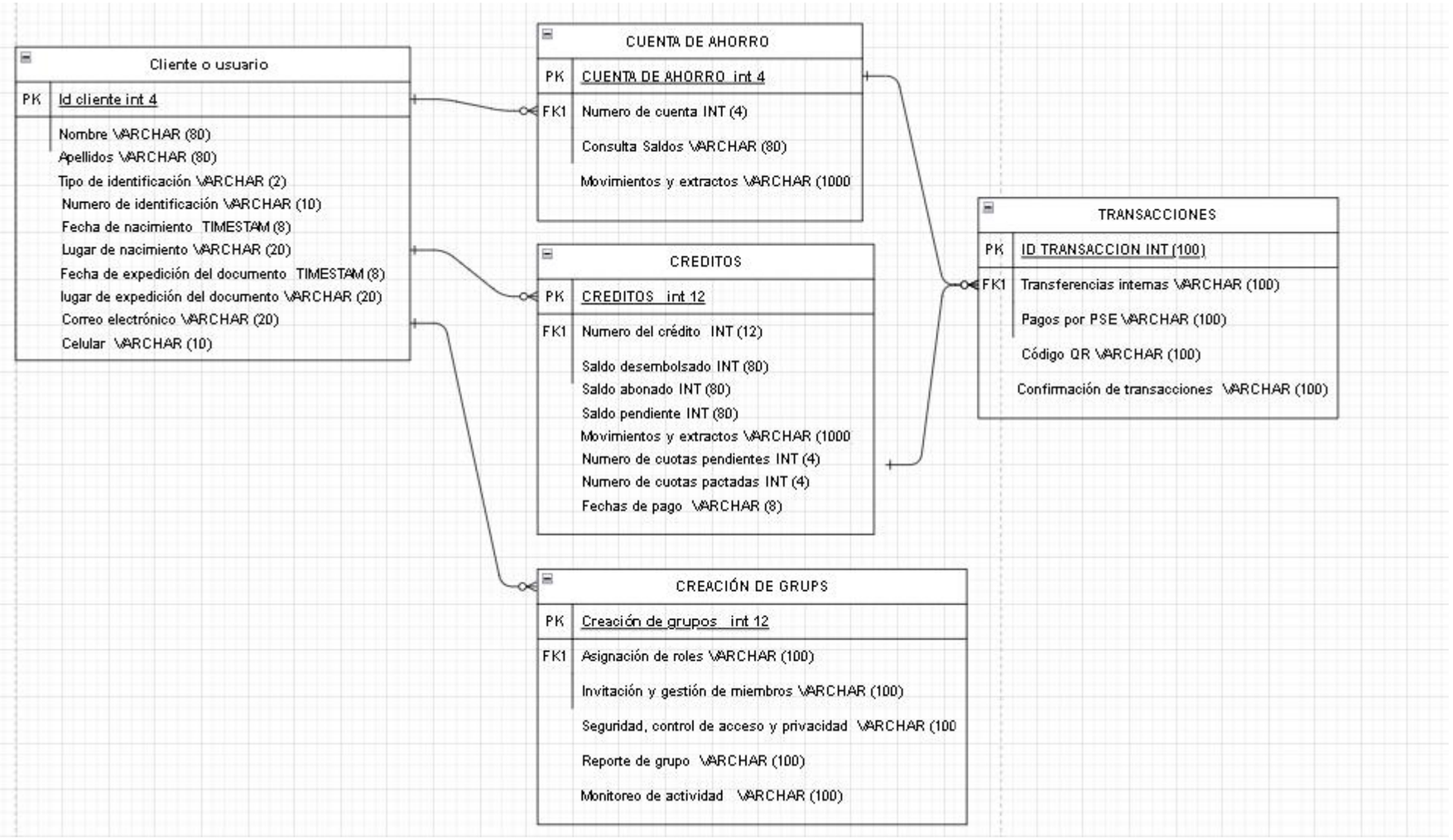
1. INTRODUCCIÓN

Este informe tiene como objetivo detallar plantear el diagrama de entidad relación y el diagrama relacional de nuestro proyecto de la aplicación web de un Bankomunal en Colombia. Nuestras comunidades necesitan un sistema de ahorro y crédito para mejorar la inclusión financiera, la transparencia y confiabilidad, nuestra aplicación tiene como objetivo modernizar la gestión de ahorros y préstamos dentro de comunidades rurales y de bajos recursos, remplazando los sistemas manuales tradicionales que se utilizan en los Bankomunales que existen actualmente.

2. DIAGRAMA ENTIDAD RELACIÓN



3. DIAGRAMA RELACIONAL



4. **DICCIONARIO DE DATOS**

Nombre	Persona		
Creación	23 de agosto del 2025		
Descripción	Registro del ingreso generados al aplicativos del Banckomunal		
CAMPO	**TIPO DE DATO**	**TAMAÑO**	**DESCRIPCIÓN**
Id persona	Int	4	identificación única de la persona en el aplicativo
Nombre	Varchar	80	Nombre del usuario
Apellidos	Varchar	80	Apellidos del usuario
Tipo de identificación	Varchar	2	
Número de identificación	Varchar	10	
Fecha de nacimiento	Timestam	8	Fecha en la que nace la persona
Lugar de nacimiento	Varchar	20	Lugar de nacimiento de la persona
Fecha de expedición del documento	Timestam	8	Fecha en la que se expide el número de identidad
Lugar de expedición del documento	Varchar	20	Lugar de expedición del documento de la persona
Correo electrónico	Varchar	20	Correo personal
Celular	Varchar	10	Teléfono personal

Nombre	Cuenta de ahorros		
Creación	23 de agosto del 2025		
Descripción	Cuenta de ahorros creada por el titular o cliente		
CAMPO	**TIPO DE DATO**	**TAMAÑO**	**DESCRIPCIÓN**
Número de cuenta	Int	4	Numero único de cuenta generado por el sistema al momento de la creación.
Consulta saldos	Varchar	80	El usuario puede visualizar el saldo de su cuenta de ahorros
Movimientos y extractos	Varchar	1000	el usuario puede visualizar todos los movimientos generados en su cuenta de ahorros

Nombre	Créditos		
Creación	23 de agosto del 2025		
Descripción	Créditos adquiridos en el banckomunal por los usuarios.		
CAMPO	**TIPO DE DATO**	**TAMAÑO**	**DESCRIPCIÓN**
Número del crédito	Int	12	Número del crédito generado por sistema al adquirir el producto.
Saldo desembolsado	int	80	El usuario puede visualizar el total desembolsado
Capital abonado	int	80	El usuario puede ver el capital abonado al crédito
Saldo pendiente	int	80	El usuario puede ver el saldo pendiente por pagar
Movimientos y extractos	Varchar	1000	el usuario puede visualizar todos los movimientos generados en los créditos adquiridos en el banckomunal
Numero de cuotas pagadas	int	4	El usuario puede visualizar el total de cuotas pagadas
Numero de cuotas pendientes	int	4	El usuario puede visualizar el total de cuotas pendientes por pagar
Fechas de pago	Timestam	8	El usuario puede visualizar las fechas de pago de sus productos

Nombre	Transacciones		
Creación	23 de agosto del 2025		
Descripción	Administrar y supervisar todas las operaciones financieras relacionadas con los usuarios		
CAMPO	**TIPO DE DATO**	**TAMAÑO**	**DESCRIPCIÓN**
Transferencias internas	Varchar	100	Permite transferir fondos entre usuarios o grupos, garantizando la validación de identidad del emisor y receptor mediante autenticación y verificación de fondos disponibles.
Pagos por PSE (pasarela de pagos)	Varchar	100	Transferencias seguras a través de PSE y soporte para múltiples métodos de pago.
Código QR	Varchar	100	Se utilizaría para pagos de préstamos, aportes a ahorros grupales o transferencias entre usuarios.
Retiros	Varchar	100	
Confirmación de transacciones	Varchar	100	Registro y control de todas las transacciones financieras, incluyendo depósitos, retiros pagos de préstamos y transferencias internas.

Nombre	Creación de grupos		
Creación	23 de agosto del 2025		
Descripción	organización y gestión de comunidades dentro de nuestro sistema		
CAMPO	**TIPO DE DATO**	**TAMAÑO**	**DESCRIPCIÓN**
Asignación de roles	Varchar	100	el creador puede asignar roles específicos a los miembros (presidente, tesorero, secretario, miembros generales), estableciendo los niveles de permisos y responsabilidades. Garantizando la validación de identidad del emisor y receptor mediante autenticación y verificación de fondos disponibles.
Invitación y gestión de miembros	Varchar	100	Permite invitar a usuarios registrados a unirse al grupo mediante invitaciones por correo electrónico. También se pueden aprobar, rechazar o eliminar miembros, así como gestionar solicitudes de ingreso.
Seguridad, control de acceso y privacidad	Varchar	100	Asegura que solo los usuarios autorizados puedan acceder a la información del grupo, utilizando autenticación robusta y permisos basados en roles. Validación de identidad para unirse a grupos mediante autenticación facial y verificación de correo electrónico. Control de acceso para que cada miembro visualice solo la información correspondiente a su rol.
Reporte de grupo	Varchar	100	Generación de reportes personalizados sobre el rendimiento financiero, contribuciones de los miembros, historial de préstamos
Monitoreo de actividad	Varchar	100	Registro de todas las actividades relevantes dentro del grupo, incluyendo cambios de roles, decisiones financieras y eventos importantes, para fines de seguimiento y auditoría.

5. INTEGRIDAD INFORMÁTICA

La integridad informática es uno de los tres principios o atributos que forman parte de la seguridad de la información, junto a la confidencialidad y la disponibilidad. La definición de integridad informática establece que los datos o información son exactos y fiables y que no han sido modificados accidentalmente o de manera intencional por terceros no autorizados, ni cuando están en reposo, en uso o en movimiento.

La integridad informática, también llamada integridad de los datos, tiene como objetivo garantizar que los datos no han sido alterados, manipulados o corrompidos y, por lo tanto, que son exactos y confiables.

Mantener la integridad informática depende tanto del hardware y el software como de los propios usuarios que tienen acceso y privilegios para manejar la información, es decir, para usar los datos, transferirlos o almacenarlos.

Para garantizar la integridad en la seguridad informática es necesario implementar medidas tanto técnicas como organizativas que eviten cualquier alteración no autorizada en los datos o información en cualquiera de sus estados y durante todo su ciclo de vida. Así, algunos ejemplos de integridad informática serían:

- El empleo de diferentes tipos de firma electrónica para verificar que el contenido de un archivo o documento no ha sido alterado y garantizar, así, por ejemplo, el no repudio de contratos firmados electrónicamente (descubre cómo tener una firma digital en enlace).
- Tener una política de copias de seguridad, que permite recuperar los datos que hayan podido verse alterados o corrompidos en un incidente de seguridad u otro tipo de desastre.
- El cifrado de bases de datos, de manera que solo las personas autorizadas puedan acceder a ellas y modificarlas.

¿Por qué es importante la integridad informática?

Cómo decíamos, la confidencialidad, integridad y disponibilidad son los tres principios de la seguridad informática y si alguno de ellos falla o no se gestiona de manera adecuada, no podríamos garantizar la exactitud y la confiabilidad de toda la información.

En el caso de la integridad informática, su importancia reside en la necesidad de tener datos correctos y de calidad para poder tomar decisiones en base a ellos. Unos datos incorrectos o alterados ofrecerán resultados incorrectos y, por tanto, inútiles para el proceso de toma de decisiones o, lo que es peor, llevarán a tomar decisiones erróneas que podrían afectar negativamente a la empresa.

Unos datos corrompidos no serán accesibles ni podrán usarse y, por lo tanto, resultarán inútiles, además, podrían suponer pérdidas para la empresa, puesto que es información que ya no puede usarse (si no se cuentan con los medios para recuperarla y restablecerla en su estado original) y podría requerir volver a invertir tiempo y recursos en su obtención.

Por otro lado, en el ámbito de la protección de datos personales, garantizar la integridad de los datos es fundamental para evitar posibles consecuencias e impacto negativo para los derechos y libertades de los interesados. Por ejemplo, en la elaboración de perfiles o decisiones automatizadas, unos datos personales incorrectos podrían derivar en un perjuicio para el interesado, como podría ser la

no concesión de un crédito o la denegación de una póliza de seguros, si su información financiera o relativa a su salud ha sido introducida de forma errónea.

Riesgos y amenazas para la integridad informática

La integridad informática puede verse amenazada por diferentes factores, tanto físicos como lógicos, que pueden provocar desde la alteración o manipulación de los datos, hasta su corrupción o su destrucción (aunque en este último caso, ya hablaríamos de un problema de disponibilidad de la información más que de integridad).

Así, entre los principales riesgos y amenazas para la integridad informática encontramos:

- El error humano, ya sea a la hora de introducir los datos, al etiquetar un archivo o base de datos, al transferir un documento o al copiarlo.
- Ciberataques cuyo objetivo es alterar o modificar la información, incluso hacerla inaccesible, como puede ocurrir en un ataque de ransomware.
- Errores provocados por fallos de hardware o software, que pueden acabar corrompiendo la información, por ejemplo, un error de disco puede corromper los archivos que haya guardados en él, haciendo que la información esté alterada o incompleta.
- Incidentes naturales o imprevisibles, como incendios, inundaciones o cortes de energía, que pueden dañar los equipos y los datos.
- Ataques internos maliciosos, es decir, personal con acceso a los datos que, por el motivo que sea, decide alterarlos o manipularlos.
- Errores que pueden producirse durante la transferencia de archivos de un dispositivo a otro que pueden resultar en la corrupción de los mismos.

¿Cómo se protege la integridad de los datos?

Existen varias medidas técnicas y organizativas que se pueden adoptar e implementar en la empresa para proteger la integridad de los datos, pero para poder llevarlas a la práctica de manera efectiva, es fundamental hacerlo a través de un plan de protección de datos informáticos o protocolo de seguridad de la información, ya que de esa forma se hará de manera planificada, realizando los correspondientes análisis de riesgos para la integridad informática, implementando las medidas de seguridad más adecuadas para minimizar la probabilidad de que ocurran y su nivel de impacto para la empresa si finalmente ocurren, así como estableciendo los controles e indicadores necesarios para llevar un seguimiento de las medidas y su eficacia, lo que permitirá, en caso de que se produzca un incidente que comprometa la integridad informática, determinar qué ha fallado y cómo puede mejorarse, para evitar que vuelva a pasar.

Algunas de las medidas de seguridad que deben figurar en esos planes o protocolos de seguridad y protección de datos, cuyo fin debe ser el de mantener la integridad informática, son las siguientes:

- Acceso restringido a la información, de manera que solo puedan acceder a ella aquellos usuarios que lo necesiten para el desempeño de sus funciones (por ejemplo, el departamento de contabilidad no tiene por qué tener

acceso a las listas de correo que usa el departamento de marketing para realizar las comunicaciones comerciales de la empresa). Así mismo, también se pueden dar permisos solo de lectura para limitar la capacidad de los usuarios para alterar o modificar la información.

- Utilizar contraseñas seguras y sensibilizar sobre su uso a los empleados, de manera que sea más difícil que personal no autorizado acceda a la información y pueda alterarla.
- Establecer controles de acceso a las instalaciones.
- Tener una política de copias de seguridad y realizarlas de manera periódica, además de hacer las debidas comprobaciones para asegurarse de que no habrá fallos en la restauración de la información que se haya visto comprometida en un incidente.
- Llevar un registro de quién accede y cuándo a la información, qué hace con ella (si se hacen modificaciones, transferencias, consultas, etc.). Este registro permite llevar un control de los accesos que se hacen a la información.
- Implementar sistema de firma digital para garantizar la integridad de la información enviada y recibida.
- Realizar auditorías internas tanto para verificar el estado de la información y comprobar que está actualizada, como para detectar fallos en el plan o protocolo de seguridad y aplicar las medidas necesarias para subsanarlos.

En definitiva, la integridad informática es un elemento fundamental de la seguridad de la información, que debemos proteger para evitar que los datos que maneja la empresa sean alterados o manipulados, lo que puede llevar a perjudicar el proceso de toma de decisiones basadas en su análisis, o corromperlos, haciéndolos inservibles.

6. BIBLIOGRAFÍA

https://protecciondatos-lopd.com/empresas/integridad-informatica/

https://zajuna.sena.edu.co/zajuna/course/view.php?id=41004