Metodología de Análisis de Riesgo
BAA

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Marzo 2014

Contenido

Nota Previa

En el marco de la emisión de las Recomendaciones en materia de Seguridad de Datos Personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto) pone a consideración de los interesados, investigadores y expertos en materia de seguridad de la información, la metodología que se desarrolla en el presente documento, a fin de recibir sus comentarios y observaciones respecto de la utilidad que tendría la misma para llevar a cabo el análisis de riesgos en el entorno del tratamiento de datos personales, así como la selección de controles de seguridad a aplicar.

Es importante señalar que esta metodología **no forma parte integral del documento de Recomendaciones en materia de Seguridad de los Datos Personales**, pues primero, es importante para el INAI, y de su especial interés, recibir las opiniones respectivas sobre la viabilidad de esta metodología, la cual fue desarrollada a petición del Instituto.

En ese sentido, la siguiente metodología de análisis de riesgo puede ser valorada por investigadores, expertos e interesados en la materia, para proponer mejoras e incluso nuevos modelos con base en los elementos que se presentan en este documento. Se considera que es una propuesta alternativa a otras metodologías basadas en los estándares y mejores prácticas referidos en las Recomendaciones en materia de Seguridad de los Datos Personales, y en ese sentido, el cumplimiento del deber de seguridad que establece el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP o Ley) dependerá de que los responsables y encargados implementen adecuadamente y mantengan a través del tiempo, los controles de seguridad necesarios para la protección de los datos personales que estén en su posesión.

Metodología de Análisis de Riesgo BAA

1. Introducción

Un acercamiento para evaluar las medidas de seguridad necesarias para proteger los activos de información es a través del análisis de riesgo, de modo que se pueda determinar cuál riesgo es más importante mitigar o cuáles activos se encuentran más expuestos.

La metodología de análisis de riesgos que se presenta en este documento se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

1) **Beneficio para el atacante.** Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).
2) **Accesibilidad para el atacante.** Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero).
3) **Anonimidad del atacante.** Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una empresa).

A partir de lo anterior, se ha dado el nombre de "BAA" a esta metodología de análisis de riesgos, lo cual tiene su origen en el **B**eneficio para el atacante, la **A**ccesibilidad para el atacante y la **A**nonimidad del atacante.

El objetivo de la metodología es realizar una clasificación de los datos personales en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección.

2. Identificación y clasificación de datos personales

Se deben identificar los **tipos de datos personales**, la **sensibilidad de los mismos** y el **número de personas** de quienes se tratan dichos datos para determinar el valor que representan para un atacante.

2.1 Clasificación de datos personales

El responsable debe identificar los tipos de datos personales que se tratan, la sensibilidad de los mismos y el número de titulares para determinar el valor de riesgo inherente de los datos para un tercero no autorizado.

Los datos personales pueden clasificarse en cuatro categorías, de acuerdo a la criticidad de los mismos por nivel de riesgo inherente:

Datos con riesgo inherente bajo
Esta categoría considera información general concerniente a una persona física identificada o identificable, que no corresponda a la información a la que refieren las otras tres categorías, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otra información que no refiera a las siguientes tres categorías.

Datos con riesgo inherente medio
Esta categoría contempla los datos que permiten conocer la *ubicación física* de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc.

También son datos de riesgo inherente medio aquéllos que permitan inferir el *patrimonio* de una persona*,* que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el *número de tarjeta bancaria de crédito* y*/o débito.*

Son considerados también, los datos de *autenticación* con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona.

Dentro de esta categoría se toman en cuenta los datos *jurídicos* tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Datos con riesgo inherente alto
Esta categoría de datos contempla a los datos personales sensibles, que de acuerdo a la Ley incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Datos con riesgo inherente reforzado
Los datos de *mayor riesgo* son los que de acuerdo a su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o

contenido en la misma, por ejemplo fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las *personas de alto riesgo* son aquéllas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional. Tratar datos de *personas de alto riesgo* involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros.

Es importante señalar que las categorías antes descritas se desarrollaron exclusivamente para la aplicación de esta metodología, y no pueden ser consideradas como un criterio emitido por el INAI. Más aún, el Pleno del Instituto no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles, podrían llegar a serlo dependiendo del contexto en que se trata la información.

2.2 Identificación de tipos de datos y de nivel de riesgo inherente

De acuerdo al punto anterior, se deberá identificar qué *tipos de datos personales* se están tratando y cuál es el *nivel de riesgo inherente* de los mismos (bajo, medio, alto, reforzado). En la Tabla 1 se presenta un ejemplo de esta identificación:

Tipo de Dato	Nivel de Riesgo Inherente
Ubicación en conjunto con patrimoniales	REFORZADO
Información adicional de tarjeta bancaria	REFORZADO
Titulares de alto riesgo	REFORZADO
Salud	ALTO
Origen, creencias e ideológicos	ALTO
Ubicación	MEDIO
Patrimoniales	MEDIO
Autenticación	MEDIO
Jurídicos	MEDIO
Tarjeta Bancaria	MEDIO
Personales de identificación	BAJO

Tabla 1. Nivel de riesgo inherente

El responsable o encargado deberá documentar los tipos de datos que tiene en tratamiento y su riesgo inherente, para uso en las siguientes secciones de la metodología. Se debe incluir todos los tipos de datos que se tiene en tratamiento.

3. Análisis de riesgos de datos personales

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

Esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales (Figura 1):

- **Beneficio**, **factor** que deriva en el nivel de **riesgo por tipo de dato**, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad**, **factor** que determina el nivel de **riesgo por tipo de acceso**, es decir, el número de accesos potenciales a los datos.
- **Anonimidad**, **factor** que determina el nivel de **riesgo por tipo de entorno** desde el que se tiene acceso a los datos.

Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

En la siguiente imagen se ilustra el procedimiento de obtención del valor de riesgo latente para los particulares:

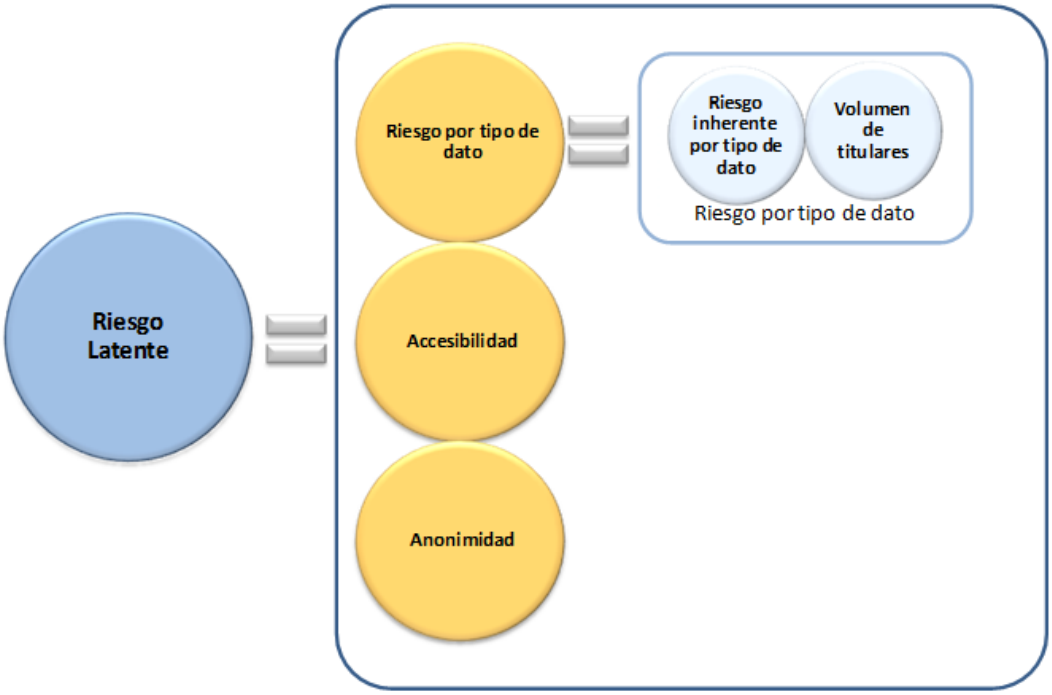

Figura 1. Cálculo de riesgo latente

3.1 Identificación de riesgo por tipo de dato

El nivel de riesgo por tipo de dato es igual al **beneficio** que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

1. Tener el nivel de *riesgo inherente de cada tipo de dato* que se trate, y;
2. Calcular el *volumen de titulares*, cuantificando el número de personas de las que se traten datos personales.

Figura 2. Identificación de riesgo por tipo de dato

El nivel de *riesgo inherente de cada tipo de dato* se determina de acuerdo a la sección **2. Identificación y clasificación de datos personales.** Mientras que el *volumen de titulares* se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

<500: Datos de hasta 500 personas
<5k: Datos entre 501 hasta 5,000 personas
<50k: Datos entre 5,001 hasta 50,000 personas
<500k: Datos entre 50,001 hasta 500,000 personas
>500k: Datos de más de 500,000 personas

Es importante que para llevar a cabo la cuantificación de titulares se consideren tanto los soportes físicos, como los electrónicos.

Se debe seleccionar uno de los rangos anteriores según el tipo de dato y su nivel de riesgo inherente, por ejemplo:

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares
Patrimoniales	**Medio**	**<50k**

3.1.1 Identificación del nivel de riesgo por tipo de dato

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de *riesgo por tipo de dato* que se trata en la organización. Se han establecido cinco niveles posibles (Figura 3) nombrados con valor numérico del 1 al 5, tal como se muestra en la siguiente imagen, donde **1** es el nivel **más bajo** y **5** el **más alto**:

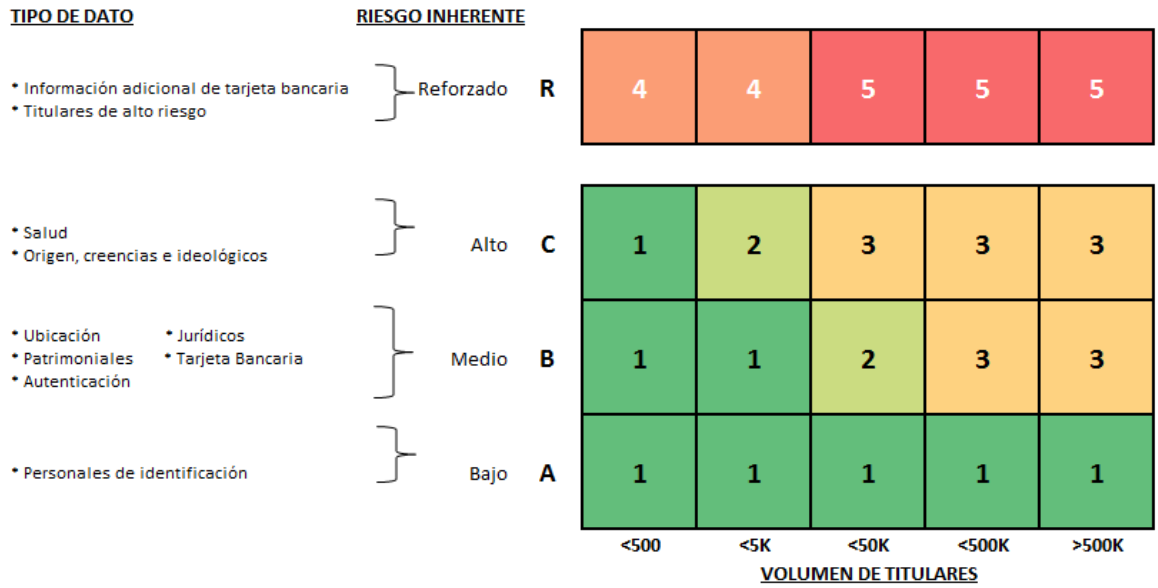

Figura 3. Nivel de riesgo por tipo de dato

A continuación se detallan los niveles mencionados:

Riesgo por tipo de dato **Nivel 1**[1], ocurre cuando:

- El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

Riesgo por tipo de dato **Nivel 2**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas
- El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas

Riesgo por tipo de dato **Nivel 3**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante
- El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante

Riesgo por tipo de dato **Nivel 4**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas

Riesgo por tipo de dato **Nivel 5**, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

[1] Ver sección Cuestionario de Autoevaluación, en la que se explica cómo identificar fácilmente si es nivel de riesgo por tipo de dato 1.

En la Tabla 2 se muestra una relación del tipo de datos con el nivel de riesgo correspondiente.

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1

Tabla 2. Nivel de riesgo por tipo de dato

Este nivel de riesgo servirá para determinar los controles que debe considerar el responsable para la protección de datos personales, que se describen en la sección relativa a la identificación de medidas de seguridad.

3.2 Cuestionario de autoevaluación

Con el objetivo de facilitar el desarrollo e implementación de la metodología para aquellos particulares cuyo nivel de riesgo sea bajo, se ha desarrollado un cuestionario de autoevaluación que permitirá efectuar un auto diagnóstico para determinar si tiene un nivel de riesgo por tipo de dato 1, el nivel de riesgo más bajo y siendo éste el caso, realizar los siguientes pasos de la metodología, con un enfoque abreviado.

Para identificar si se tiene nivel de riesgo por tipo de dato 1, se debe responder los siguientes cuestionamientos:

Los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita identificar la ubicación del titular.

1. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos que permiten inferir el patrimonio del titular, que incluyen entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados.

2. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos de autenticación son información referente a los usuarios y contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, copia de identificaciones oficiales y cualquier otro que permita autenticar al titular.

3. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos dentro de los expedientes jurídicos, penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido de forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

4. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

El número de tarjeta bancaria o de crédito conformado por los 15 o 16 dígitos únicos de la tarjeta de crédito y/o débito.

5. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

De acuerdo a la LFPDPPP, los datos sensibles incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasada, presente o futura; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular. Para efectos del presente documento los datos sensibles serán considerados datos de alto riesgo.

6. ¿De los datos sensibles descritos en este punto; obtiene, usa, divulga o almacena datos de más de 500 personas?

SI NO

Los datos *reforzados* son los que de acuerdo a su naturaleza tienen un nivel superior de riesgo, derivado del beneficio económico o reputacional que pueda representar para un tercero. A continuación se listan los datos de mayor riesgo:

De ubicación en conjunto con patrimoniales: Aquéllos que relacionen datos patrimoniales con ubicación física del titular.

Información adicional de tarjeta bancaria: el número tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, código de seguridad (CVV, CVV2, CAV2, CVC2, CID), datos de banda magnética o número de identificación personal (PIN).

7. ¿Obtiene, usa, divulga o almacena datos correspondientes a los descritos en este punto?

SI NO

Los *titulares de alto riesgo* son las personas que debido a su oficio, profesión o naturaleza están expuestos a una mayor probabilidad de ser atacados debido al beneficio económico o reputacional que sus datos pueden representar para un tercero. Por lo tanto, el tener datos de estos titulares eleva el riesgo de la información de la base de datos completa y en consecuencia para todas las personas contenidas en ella. Los titulares de alto riesgo incluyen líderes políticos, religiosos, empresariales, de opinión, de impartición de justicia, responsables de seguridad nacional y cualquier otra persona que sea considerada como personaje público.

8. ¿Obtiene, usa, divulga o almacena datos de titulares de alto riesgo?

SI NO

Si todas las respuestas a las preguntas anteriores fueron “NO”, entonces los controles de seguridad que deberá implantar en los sistemas que traten, procesen o guarden datos personales, corresponden al **nivel mínimo requerido,** y deberá implantar la lista básica de medidas de seguridad (Lista 1). Esto mismo lo puede corroborar siguiendo los pasos de la metodología simple.

En el **ANEXO A** *Mecanismo de autoevaluación* se encuentra contenido el cuestionario de autoevaluación y algunos pasos acotados para el nivel de riesgo por tipo de dato 1.

Si al menos una de las respuestas fue “SÍ”, deberá implantar medidas de controles de seguridad mayores al nivel mínimo y continuar con las secciones siguientes de este documento.

3.3 Identificación de nivel de accesibilidad

Una vez obtenido el factor **Beneficio**, es decir el nivel de *riesgo por tipo de dato*, es necesario identificar el nivel de *riesgo por tipo de acceso*, (Tabla 3). Se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, es decir, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información.

Accesibilidad (Cantidad de accesos a los datos personales)
≤ 20
> 20 ≤ 200
> 200 ≤ 2,000
> 2,000

Tabla 3. Umbrales de nivel de accesibilidad

3.4 Identificación de nivel de anonimidad

Después de obtener el factor **Accesibilidad**, se debe identificar qué tan anónimos son los accesos a la información; es decir, el nivel de *riesgo por tipo de entorno*. Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la organización, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

En la siguiente tabla se listan los entornos de acceso en una escala del 1 al 5, en donde **1** implica **baja anonimidad** y **5 mayor anonimidad** del atacante, es decir, entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.

Entorno	Nivel de Anonimidad
Físico	1
Red interna	2
Red inalámbrica	3
Red de terceros	4
Internet	5

Tabla 4. Nivel de anonimidad

Se deberá seleccionar el nivel aplicable para cada tipo de dato en tratamiento. En caso de que los datos se accedan desde más de un entorno, se deberá considerar el entorno de mayor riesgo por cada tipo de dato. Esto se utilizará en la sección Identificación de Medidas de Seguridad.

A continuación (Figura 4) se presenta un esquema de los entornos digitales:

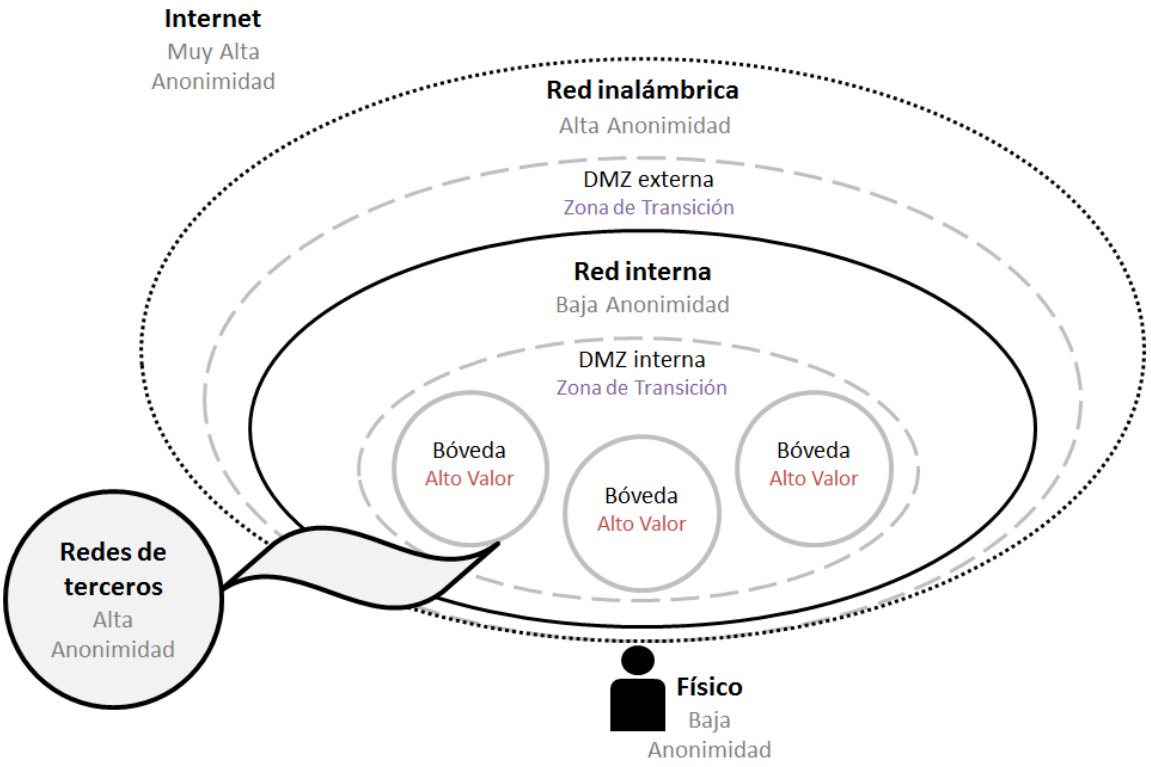

Figura 4. Entornos de acceso

3.5 Identificación de nivel de riesgo latente

La combinación de los tres factores analizados; nivel de *riesgo por tipo de dato* (**beneficio**), nivel de *riesgo por tipo de acceso* (**accesibilidad**) y nivel de *riesgo por tipo de entorno* (**anonimidad**), da como resultado el nivel de **riesgo latente** que presenta cada organización (Figura 5).

Figura 5. Nivel de riesgo latente

4. Identificación de medidas de seguridad

Una vez obtenido el nivel que le corresponde a cada factor de riesgo, se deben identificar las medidas de seguridad aplicables a la organización. Para ello, se desarrollaron cinco tablas matriciales que combinan el nivel de riesgo por tipo de dato, el nivel de accesibilidad y el nivel de anonimidad, dando como resultado un patrón de control o lista de controles a implantar.
Se han definido listas y patrones de control que agrupan medidas de seguridad basadas en ISO/IEC 27002:

- **Listas de controles.** Utilizaremos este término para describir la situación en la que no es imperante implantar todos los controles sugeridos, sino que existirán medidas necesarias y medidas opcionales para que el responsable de seguridad seleccione aquéllas que, sumadas, apoyan a la mitigación del riesgo existente en el contexto de su organización. Es decir, en el caso de las listas, la suma de controles contribuye a la protección de la información, teniendo la posibilidad de seleccionar uno a más controles.
  Existen listas de controles administrativos, de seguridad física y del entorno de red interna.

- **Patrones de control.** Utilizaremos este término para describir la situación en la que, de acuerdo a la situación de riesgo identificada, es necesario implantar en su totalidad los controles descritos dentro del mismo. Los patrones de control existentes son: Controles Básicos, DMZ y Caja Fuerte (entorno recomendado para resguardar información con nivel de riesgo por tipo de dato 4 y 5). Sólo se podrá descartar alguna medida de seguridad en el caso de que no sea aplicable a su infraestructura, por ejemplo, un control enfocado a comercio electrónico se podrá descartar sólo si la organización no cuenta con dicha actividad.

Como se mencionó al inicio de la sección se cuenta con cinco tablas, cada tabla corresponde a un nivel de riesgo por tipo de dato (1 al 5); dentro de las tablas, en las filas se encuentra mapeado matricialmente el nivel de anonimidad (representado por el entorno de acceso a los datos), y en las columnas el nivel de accesibilidad (representado por el número de personas o accesos a los datos). En las celdas de dichas tablas se encuentran distribuidos los patrones de control y las listas de medidas de seguridad a implantar. Asimismo, para el nivel de riesgo por tipo de dato “1”, se definió un conjunto de medidas básicas de seguridad que aplica a todas las combinaciones de anonimidad y accesibilidad, estas medidas de seguridad son las mínimas necesarias y no contempla controles opcionales; esto no exime al responsable o encargado de implementar más controles si fuera necesario.

Se han definido tres tipos de patrones y tres tipos de listas, cada uno de ellos con niveles que atienden a diferentes combinaciones de riesgo.

Patrones de control:

1. CB: Patrón de control de medidas de seguridad básicas. Es aplicable para aquellos particulares cuyo nivel de riesgo por tipo de dato es igual a 1.

2. DMZ: Patrón para accesos desde entornos de alta anonimidad. Hace referencia a la necesidad de implementar una zona desmilitarizada como zona de transición entre un

entorno de mayor riesgo y uno de menor riesgo. Se contemplan dos niveles de este patrón.

   a. DMZ 2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad.
   b. DMZ 3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad.

3. CF: Patrón aplicable para datos de nivel 4 y 5 de riesgo por tipo de dato. Su nombre hace referencia a las iniciales de Caja Fuerte, debido a que se recomienda que estos tipos de datos se aíslen y se protejan con medidas de seguridad mucho más estrictas y se construya una "caja fuerte" alrededor de ellos, para protegerlos de accesos no autorizados. Se contemplan dos niveles para este patrón.
   a. CF 1. Patrón de control de medidas de seguridad para caja fuerte nivel 1.
   b. CF 2. Patrón de control de medidas de seguridad para caja fuerte nivel 2.

Listas de medidas de seguridad:

1. AD: Lista de medidas administrativas. Esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista.
   a. AD-2. Medidas administrativas para nivel de riesgo por tipo de dato 2.
   b. AD-3. Medidas administrativas para nivel de riesgo por tipo de dato 3.
   c. AD-4-5. Medidas administrativas para nivel de riesgo por tipo de dato 4 o 5.

2. RI: Lista de medidas de seguridad aplicable para accesos desde la red interna. Esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su red interna. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse en la red.
   a. RI 1. Medidas básicas de seguridad para accesos desde red interna.
   b. RI 2. Medidas intermedias de seguridad para accesos desde red interna.
   c. RI 3. Medidas reforzadas de seguridad para accesos desde red interna.

3. F: Lista de medidas de seguridad aplicable para accesos desde el entorno físico. Esta lista contiene controles de seguridad física necesarios y opcionales. Se cuenta con tres niveles para esta lista.
   a. FI 1. Medidas básicas de seguridad para accesos físicos.
   b. FI 2. Medidas intermedias de seguridad para accesos físicos.
   c. FI 3. Medidas reforzadas de seguridad para accesos físicos.

En el Anexo B: Medidas de Seguridad, se encuentran las listas y patrones de control propuestos.

4.1 Tablas de control

A continuación se muestran las cinco tablas mencionadas:

Tabla 1: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 1. Para todas las combinaciones de esta tabla le corresponde el patrón de control de medidas básicas de seguridad (CB), mismo que deberá aplicarse en su totalidad.

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 1. Riesgo por tipo de dato 1

Tabla 2: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 2.

		Riesgo por tipo de dato 2			
		Medidas administrativas aplicables: AD-2			
Entornos de acceso	**Internet**	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red terceros	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	WiFi	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red interna	RI-1 F-1	RI-1 F-1	RI-2 F-2	RI-2 F-2
	Físico	F-1	F-1	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de control 2. Riesgo por tipo de dato 2

Tabla 3: Es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 3.

Entornos de acceso		Medidas administrativas aplicables: AD-3			
	Internet	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red terceros	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	WiFi	RI-2 F-2 DMZ-2	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red interna	RI-2 F-2	RI-3 F-2	RI-3 F-2	RI-3 F-2
	Físico	F 2	F 2	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de control 3. Riesgo por tipo de dato 3

Tabla 4: es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 4.

		Riesgo por tipo de dato 4			
		Medidas administrativas aplicables: AD-4-5			
Entornos de acceso	Internet				
	Red terceros				
	WiFi				
	Red interna	F-3 CF-1	F-3 CF 1	F-3 CF 1	F-3 CF-2
	Físico	F-3	F-3	F-3	F-3
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 4. Riesgo por tipo de dato 4

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos contra entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, internet o redes inalámbricas.

Tabla 5: Es la tabla que deberán utilizar los particulares cuyo nivel de riesgo por tipo de dato es 5.

		Riesgo por tipo de dato 5			
		Medidas administrativas aplicables: AD-4-5			
Entornos de acceso	Internet				
	Red terceros				
	WiFi				
	Red interna	F-3 CF-1	F-3 CF-2	F-3 CF-2	F-3 CF-2
	Físico	F 3	F 3	F 3	F 3
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 5. Riesgo por tipo de dato 5

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, internet o redes inalámbricas.

4.2 Procedimiento de selección de medidas de seguridad

A continuación se describe el procedimiento para identificar la lista de medidas de seguridad o patrón de control a implantar, tomando como base el nivel de riesgo que se obtuvo en la sección "Análisis de riesgos de los datos personales".

Para el uso de las tablas se deben realizar los siguientes pasos:

1. De acuerdo con el nivel de riesgo por tipo de dato, identificar la tabla que le corresponde. Si se obtuvo riesgo por tipo de dato igual a 1, independientemente del entorno de acceso y el número de accesos que se tengan, le corresponde implementar el patrón de control de medidas básicas de seguridad. Si obtuvo un nivel de riesgo por tipo de dato mayor a 1 continuar con los siguientes pasos.
2. Seleccionar la fila con el entorno de accesos a los datos personales de mayor riesgo, identificado en la sección de identificación de nivel de anonimidad.
3. Seleccionar la columna con el rango de accesos identificado en la sección de identificación de nivel de accesibilidad.
4. Identificar la celda de la matriz en la cual se cruzan la columna y la fila seleccionadas.
5. Identificar la lista o patrón de control que le corresponde aplicar de acuerdo a su nivel de riesgo. Nótese que existen casos en los que además de implementar un patrón de control se deberá implementar una lista de red interna y una lista de acceso físico.

La aplicación de controles en cada entorno deberá ser exhaustiva y deberá cubrir las necesidades de anonimidad, accesibilidad y riesgo por tipo de dato pertinentes para cada tipo de dato personal recabado. De acuerdo con el criterio del responsable o encargado, si así se desea, se pueden implementar más controles que los recomendados.

El patrón de control y las listas de medidas de seguridad correspondientes al nivel de riesgo serán la base con la que se trabajará en el análisis de brecha.

Ejemplo:

Si en el análisis de riesgos se identificó que se cuenta con datos de salud de más de 50,000 titulares, y por lo tanto le corresponde un nivel de riesgo por tipo de dato 3, se deberá seleccionar la tabla 3. Con ello se identifica que le corresponde la lista de medidas administrativas AD-3.

Siguiendo con el ejemplo, decimos que en el análisis de riesgos se identificó que se tienen menos de doscientos accesos a los datos personales y que estos accesos son desde la red interna, el entorno físico y redes de terceros.

Por lo tanto se debe seleccionar la celda que cruza la fila de red de terceros (entorno de mayor anonimidad en este ejemplo) con el rango de accesos menor o igual a 200.

		Medidas administrativas aplicables: AD-3			
Entornos de acceso	**Internet**	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red terceros	RI-2 F-2 DMZ-3	**RI-3 F-2 DMZ-3**	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	WiFi	RI-2 F-2 DMZ-2	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red interna	RI-2 F-2	RI-3 F-2	RI-3 F-2	RI-3 F-2
	Físico	F 2	F 2	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de controles 3. Riesgo por tipo de dato 3

La celda seleccionada indica que se deberá implementar:

- el patrón DMZ-3,
- la lista de medidas de seguridad de red interna RI-3,
- la lista de medidas de seguridad para acceso físico F-2;
- esto además de la lista de medidas administrativas AD-3.

Es importante tomar en cuenta que este ejercicio se debe hacer por cada tipo de dato.

5. Optimización de los niveles de riesgo

Existen acciones que se pueden implementar en la metodología BAA para disminuir el riesgo latente de los datos y así reducir el nivel de seguridad requerido, como las que se muestran a continuación:

Disociar la información

Por medio de la correcta aplicación del control de disociación se despersonalizan los datos y con ello se minimiza el riesgo para las personas, logrando así que ya no sean identificables. Es decir, cuando los datos se aíslan de manera que por sí mismos no aporten información valiosa o no puedan volver identificable a una persona, entonces se considera que la información está disociada. Para que dicho mecanismo sea efectivo es necesario contar con autenticaciones distintas para acceder a los diferentes datos aislados.

Separación de la información
Separando la información en bases de datos de menor tamaño ayuda a disminuir el riesgo que representan, pues mientras mayor cantidad de datos tenga una sola base de datos, la probabilidad de que un atacante tenga interés en ella se incrementa. Es necesario considerar que para que el control de separación sea efectivo, no debe existir ningún acceso por medio del cual se pueda acceder al total de información, es decir, es necesario que cada base de datos requiera una autenticación distinta.

Incluir datos de menor riesgo en la caja fuerte. Debido a que el nivel de protección de la red interna está determinado por el dato con mayor nivel de riesgo, existen casos en los que, implementar los controles de protección requeridos a lo largo de la red es costoso. Una estrategia recomendada para disminuir los costos de protección es aislar los datos de menor riesgo dentro de la caja fuerte, bajando automáticamente el nivel de protección requerido para la red interna.
Es recomendable analizar los costos de tomar esta medida o no, para tomar la opción que le brinde mayor eficiencia en la implementación de las medidas.

Reducción de accesibilidad
Disminuir la cantidad de accesos a los datos personales contribuye a la reducción del riesgo latente de los datos, por lo tanto se recomienda analizar si todos los accesos a los datos personales son necesarios, para llevar a cabo una depuración de los mismos. Con esta acción bajamos el nivel de riesgo y con ello el nivel de protección requerido.

Eliminar entornos de acceso
Existen entornos de acceso que suponen un nivel de riesgo mayor pues presentan niveles de anonimidad alta, por lo que descartar el acceso a los datos personales desde entornos que no sean específicamente necesarios aporta a la disminución del riesgo latente de los datos personales.

6. Inventario de datos y sistemas de tratamiento

Se deben inventariar los soportes físicos (archivos, gavetas, entre otros) y electrónicos (sistemas, aplicaciones, bases de datos, entre otros) donde se tratan los datos personales.

La organización debe identificar exclusivamente aquellos sistemas de tratamiento que manejan datos personales. Todos aquellos sistemas de tratamiento que no manejan datos personales, no están en el alcance de este procedimiento y para fines del presente no es necesario inventariarlos.

Por cada uno de los datos personales identificados, se deben identificar los soportes físicos, tales como archiveros, gavetas, anaqueles y bodegas en los cuales se procesan y almacenan dichos datos. En el mismo sentido se deben identificar los soportes electrónicos, tales como aplicaciones, bases de datos, unidades de almacenamiento, equipos y toda aquella infraestructura tecnológica en los cuales se procesan y almacenan dichos datos.

Para desarrollar el inventario, se recomienda tomar en cuenta los siguientes:

- Si se obtuvo un nivel de riesgo por tipo de dato igual a 1, 2 o 3, entonces:
    - El inventario de datos es simple, es suficiente enlistar los sistemas de tratamiento físico o electrónico.

- Si se obtuvo un nivel de riesgo por tipo de dato igual a 4 o 5, entonces:
    - Se recomienda realizar un inventario de sistemas físicos y electrónicos con mayor nivel de detalle donde se tratan los datos personales y sensibles.

El inventario debe considerar los tipos de datos personales y sensibles que se tratan, y recabar al menos la siguiente información:

Sistemas de tratamiento físico

- **Lista de soportes físicos.** Enlistar y describir los soportes físicos donde se almacenan los datos, por mencionar algunos: gavetas, archiveros, bóvedas de documentación histórica, cajas de documentación, entre otra.
- **Número de soportes físicos.** Enumerar la cantidad o volumen de soportes físicos.

Sistemas de tratamiento electrónico

- **Lista de aplicaciones.** Enlistar y describir las aplicaciones a través de las cuales se tratan los datos, por ejemplo ERP´s, sistemas legados, paquetes de software, entre otros.
- **Número de aplicaciones.** Enumerar la cantidad o volumen de aplicaciones desde donde se traten datos.
- **Lista de servidores / equipos.** Enlistar y describir los servidores físicos o virtuales desde donde se tratan datos, considerar las bases de datos, servidores de archivos, servidores de aplicación, entre otros.
- **Número de servidores / equipos.** Enumerar la cantidad o volumen de servidores o equipos que traten los datos.

7. Resumen de la metodología

El objetivo final de esta metodología es determinar los controles recomendados de protección de datos de acuerdo al entorno de riesgo existente. Por lo tanto, estas listas de controles se identificarán al final, utilizando tres factores:

- Riesgo por tipo de dato (beneficio);
- Nivel de accesibilidad, y
- Nivel de anonimidad.

Los pasos a seguir son:

1. Identificar el riesgo por tipo de dato, de acuerdo con los datos personales que se tratan (nivel de riesgo inherente).
2. Con el número identificado en la primera tabla (nivel de riesgo inherente), se procede a buscar la tabla que le corresponde a ese número, para en ella utilizar como coordenadas las otras dos variables: accesibilidad y anonimidad.
3. Utilizando el grado de accesibilidad y anonimidad, es decir, desde dónde se accede a los datos (anonimidad) y qué cantidad de accesos existen (accesibilidad), se identifica la celda correspondiente en la cual se identificarán los patrones de controles que se requiere implantar.

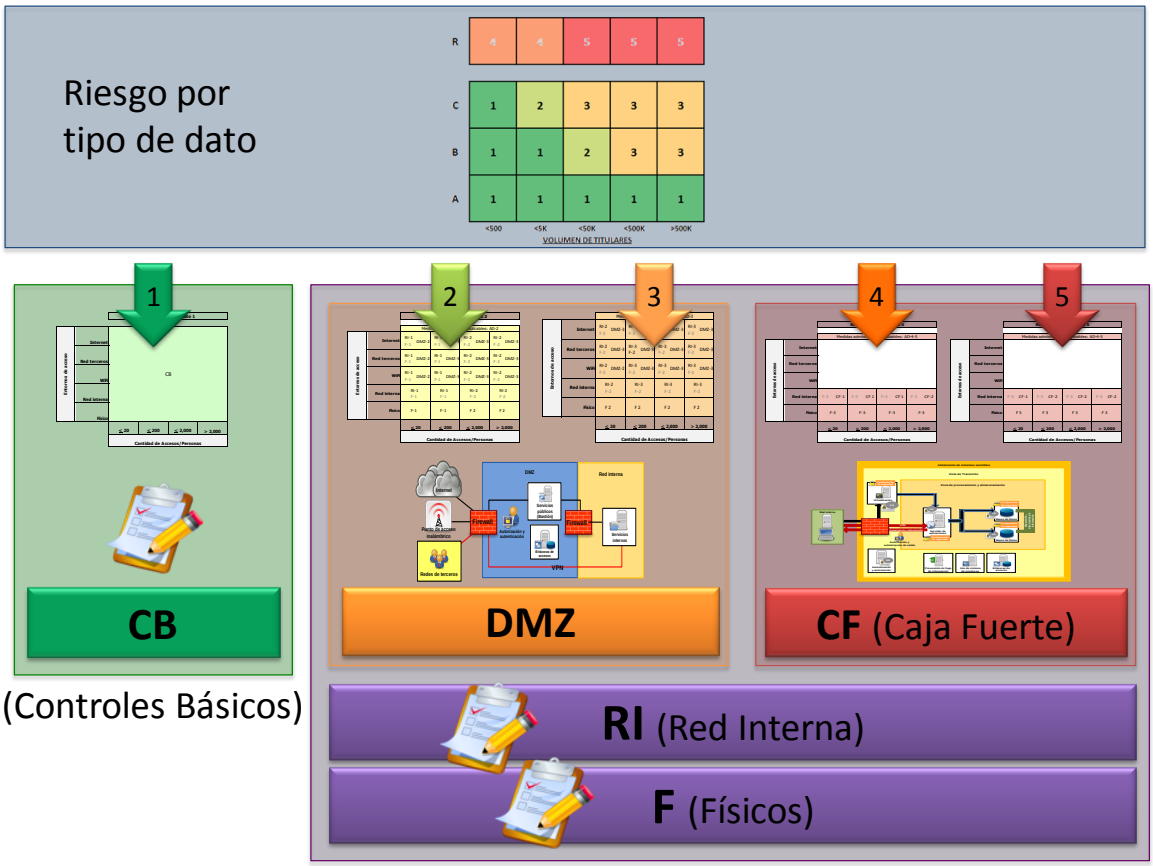

Figura 6. Resumen de la metodología

ANEXO A. MECANISMO DE AUTOEVALUACIÓN

Razón social:	
Dirección:	
Actividad comercial:	
Fecha de elaboración:	

Obtener, usar, divulgar o almacenar datos personales es legítimo, sin embargo la seguridad en el contexto de la Ley busca prevenir el mal uso y el acceso no autorizado a estos datos.

Este mecanismo le permitirá llevar acabo un autodiagnóstico para determinar su nivel de riesgo de acuerdo con los datos personales que obtiene, usa, divulga o almacena. A partir del nivel de riesgo identificado se recomendará el conjunto de controles aplicables. Se recomienda llevar a cabo el ejercicio de resolución del mecanismo de autoevaluación por lo menos de forma anual.

Se deberá entender como datos personales cualquier información concerniente a una persona física identificada o identificable, como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, dependientes, beneficiarios y familiares, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, referencias laborales, referencias personales, información migratoria y cualquier otro dato que pudiera identificar o hacer identificable al titular.

¿Obtiene, usa, divulga o almacena información concerniente a una persona física identificada o identificable?

○ SI ○ NO

En el caso de haber contestado “NO”, entonces no tiene la obligación de cumplir con lo dispuesto en la Ley. En caso contrario se deberá continuar con la sección 1 y 2.

NOMBRE	FECHA	FIRMA

Sección 1: Cuestionario de autoevaluación sobre tipo de datos personales y volumen de personas

Datos de nivel de riesgo medio:

Los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país y/o cualquier otro que permita identificar la ubicación del titular.

1. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos que permiten inferir el patrimonio del titular, que incluyen entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados.

2. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos de autenticación son información referente a los usuarios y contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, copia de identificaciones oficiales y cualquier otro que permita autenticar al titular.

3. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Los datos dentro de los expedientes jurídicos, penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido de forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

4. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

El número de tarjeta bancaria o de crédito conformado por los 15 o 16 dígitos únicos de la tarjeta de crédito y/o débito.

5. ¿De los datos descritos en este punto; obtiene, usa, divulga o almacena datos de más de 5,000 personas?

SI NO

Datos de nivel de riesgo alto:

De acuerdo con la LFPDPPP, los datos sensibles incluyen los datos sensibles incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasada, presente o futura; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular. Para efectos del presente documento los datos sensibles serán considerados datos de alto riesgo.

6. ¿De los datos sensibles descritos en este punto; obtiene, usa, divulga o almacena datos de más de 500 personas?

○ SI ○ NO

Datos reforzados:

Los datos ***reforzados*** son los que de acuerdo a su naturaleza tienen un nivel superior de riesgo, derivado del valor económico o reputacional que pueda representar para un tercero. A continuación se listan los datos de mayor riesgo:

De ubicación en conjunto con patrimoniales: Aquellos que relacionen datos patrimoniales con ubicación física del titular.

Información adicional de tarjeta bancaria: el número tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma, por ejemplo fecha de vencimiento, código de seguridad (CVV, CVV2, CAV2, CVC2, CID), datos de banda magnética o número de identificación personal (PIN).

7. ¿Obtiene, usa, divulga o almacena datos correspondientes a los descritos en este punto?

○ SI ○ NO

Los ***titulares de alto riesgo*** son las personas que debido a su oficio, profesión o naturaleza están expuestos a una mayor probabilidad de ser atacados debido al valor económico o reputacional que sus datos pueden representar para un tercero. Por lo tanto, el tener datos de estos titulares eleva el riesgo de la información de la base de datos completa y en consecuencia para todas las personas contenidas en ella. Los titulares de alto riesgo incluyen líderes políticos, religiosos, empresariales, de opinión, de impartición de justicia, responsables de seguridad nacional y cualquier otra persona que sea considerada como personaje público. Recomendamos que se mantenga un nivel elevado de protección de los datos de los titulares descritos en el párrafo anterior.

8. ¿Obtiene, usa, divulga o almacena datos de titulares de alto riesgo?

○ SI ○ NO

Si todas las respuestas a las preguntas anteriores fueron “NO”, entonces los controles de seguridad que deberá implantar en los sistemas que traten, procesen o guarden datos personales corresponde al **nivel mínimo requerido** y deberá continuar con la sección 2 de este anexo.

Si al menos una de las respuestas fue “SÍ”, deberá implantar controles de seguridad mayores a las estipuladas en este anexo.

Con el objetivo de simplificar la operación y administración de las medidas de seguridad para el nivel de riesgo por tipo de dato “1”, se recomienda la documentación e implementación de un Contrato de Adhesión (CDA), que conjunte de forma sencilla los controles y funja como una lista de control de accesos a los datos personales. El CDA se incluye en la siguiente sección del presente anexo.

Sección 2: Contrato de Adhesión (CDA).

Si después de haber contestado el cuestionario de autoevaluación la sección 1, se determinó que el nivel de seguridad aplicable es el **mínimo requerido,** de acuerdo con los datos personales que se obtienen, usan, divulgan o almacenan; entonces se recomienda implementar el patrón de control básico (ver ANEXO B), o el CDA mismo que mantiene de forma simplificada los controles incluidos en el patrón mencionado.

1. **Personal autorizado**. A continuación enliste las personas autorizadas para obtener, usar, divulgar, almacenar o acceder a los datos personales.

Nombre Completo	Función	Fecha inicio	Fecha fin	Firma

1.1. El personal interno o externo que interviene en el tratamiento de los datos personales tiene, entre otras, las siguientes obligaciones:
- Resguardar la confidencialidad de los datos personales a los que se tiene acceso.
- Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos en el exterior.
- Leer el CDA y firmarlo aceptando el entendimiento de las obligaciones que tiene respecto a la protección de los datos personales.

1.2. Responsabilidades de Seguridad:
Todos los empleados, contratistas y terceros deben cumplir con las medidas de seguridad dispuestas para la protección de los datos personales y hacer uso de los datos personales únicamente para la función para la que fue autorizada.

1.3. Sanciones:
La divulgación o uso no autorizado de los datos personales podrán ser sancionados conforme a lo estipulado en el capítulo X de la LFPDPPP.

2. El CDA deberá ser llenado y actualizado anualmente para asegurar que el tratamiento de los datos personales no ha cambiado y se mantienen las medidas de protección de los mismos.

3. Se debe garantizar que las bases de datos personales, tanto físicas, como electrónicas, mantienen las siguientes medidas de seguridad:

Medida de seguridad	Indicar si se tiene implementado (SI / NO)	Fecha de implementación (sólo si es posterior a la generación inicial del CDA)
Control de acceso por medio de contraseña, llave, cerradura.		

Protector de pantalla con solicitud de contraseña para desbloqueo.		
Mecanismos contra código malicioso.		
Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto.		
Establecer contraseña a la red inalámbrica.		
Instalar actualizaciones de seguridad en los equipos de forma semestral		

3.1. Registrar los soportes físicos (p.e.: archiveros, entre otros) o electrónicos (p.e.: computadoras portátiles o de escritorio, discos duros, servidores de archivos, aplicaciones, etc.) donde se traten datos personales.

Soportes físicos

ID Soporte	Nombre de Soporte Físico	Ubicación
1	*Archivero de documentos "A"*	

Sistemas electrónicos

ID Soporte	Nombre de Soporte Electrónico
1	*Sistema "A"*
2	*Computadora de escritorio "a"*
3	*Computadora de escritorio "b"*

3.2. Se debe garantizar la eliminación de los accesos otorgados al vencimiento de la fecha o rango autorizado. El activo o llave otorgados para llevar a cabo las funciones deben ser devueltos.

3.3. Protección de equipo: El equipo debe estar situado de forma que se eviten accesos no autorizados.

4. Cuando el tratamiento de la información ya no sea necesario, se debe:
    - Garantizar la destrucción de los medios físicos que contengan datos personales, de tal forma que no sea posible reconstruirlos.
    - Garantizar el borrado de la información en bases de datos lógicas que contengan datos personales, de tal forma que no sean fácilmente recuperables.

Aunado a los controles mencionados anteriormente, se debe poner en práctica un programa de capacitación, actualización y concienciación del personal sobre las obligaciones en materia de protección de datos personales, como lo indica el artículo 68 del Reglamento de la LFPDPPP. Asimismo, el responsable debe cumplir con todos los principios y deberes que establece la LFPDPPP, su Reglamento y normativa aplicable.

NOMBRE DEL RESPONSABLE DE LOS DATOS PERSONALES	**FECHA**	**FIRMA**

ANEXO B. MEDIDAS DE SEGURIDAD

En el presente anexo se encuentran los patrones de control y las listas de medidas de seguridad definidas para las combinaciones disponibles de riesgo por tipo de dato, accesibilidad y anonimidad. Los controles (medidas de seguridad) fueron seleccionados de las mejores prácticas, como ISO 27002.

Es importante señalar que implantar un grupo de controles tiene más beneficio que la selección e implantación de controles de manera individual, ya que la conjunción de los mismos representa en cierta medida una acumulación de las capacidades de mitigación de riesgos y protección de información.

Para apoyar a la identificación del grupo de medidas de seguridad que le corresponde de acuerdo a su nivel de riesgo se definieron cinco tablas matriciales, una por cada nivel de riesgo por tipo de dato, en las que las filas son los entornos de acceso a los datos y las columnas son los umbrales de accesos potenciales a los datos.

Para determinar la lista o patrón correspondiente, se deberán seguir los siguientes pasos:

- Identificar la tabla que le corresponde de acuerdo con el nivel de riesgo por tipo de dato que se obtuvo en el análisis de riesgos.
- Una vez que se encuentre posicionado en la tabla que le corresponde, identificar el rango de accesos potenciales que se tiene para cada tipo de dato y el entorno de acceso de máxima anonimidad desde el que se accede a los datos. La celda que cruza en las filas y columnas corresponde al patrón de control o lista de controles a implantar.

Para más detalle ver la sección de identificación de medidas de seguridad.

A continuación se presentan las cinco tablas disponibles:

Tabla 1: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 1.

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 1. Riesgo por tipo de dato 1

Tabla 2: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 2.

		Riesgo por tipo de dato 2			
		Medidas administrativas aplicables: AD-2			
Entornos de acceso	**Internet**	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red terceros	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	WiFi	RI-1 F-1 DMZ-2	RI-1 F-1 DMZ-3	RI-2 F-2 DMZ-3	RI-2 F-2 DMZ-3
	Red interna	RI-1 F-1	RI-1 F-1	RI-2 F-2	RI-2 F-2
	Físico	F-1	F-1	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de control 2. Riesgo por tipo de dato 2

Tabla 3: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 3.

		Medidas administrativas aplicables: AD-3			
Entornos de acceso	**Internet**	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red terceros	RI-2 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	WiFi	RI-2 F-2 DMZ-2	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3	RI-3 F-2 DMZ-3
	Red interna	RI-2 F-2	RI-3 F-2	RI-3 F-2	RI-3 F-2
	Físico	F 2	F 2	F 2	F 2
		≤ 20	**≤ 200**	**≤ 2,000**	**> 2,000**
		Cantidad de Accesos/Personas			

Tabla de control 3. Riesgo por tipo de dato 3

Tabla 4: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 4.

		Riesgo por tipo de dato 4			
		Medidas administrativas aplicables: AD-4-5			
Entornos de acceso	Internet				
	Red terceros				
	WiFi				
	Red interna	F-3 CF-1	F-3 CF 1	F-3 CF 1	F-3 CF-2
	Físico	F-3	F-3	F-3	F-3
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 4. Riesgo por tipo de dato 4

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, Internet o redes inalámbricas.

Tabla 5: Deberá ser utilizada por los particulares cuyo nivel de riesgo por tipo de dato es 5.

		Riesgo por tipo de dato 5			
		Medidas administrativas aplicables: AD-4-5			
Entornos de acceso	Internet				
	Red terceros				
	WiFi				
	Red interna	F-3 CF-1	F-3 CF-2	F-3 CF-2	F-3 CF-2
	Físico	F 3	F 3	F 3	F 3
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

Tabla de control 5. Riesgo por tipo de dato 5

Nótese que no se encuentran disponibles algunas de las combinaciones de umbral de accesos vs. entorno de acceso; esto se debe a que son escenarios que implicarían un nivel de riesgo muy alto y no se recomienda que existan. En caso de que su organización presente estos escenarios es necesario que impida que se presenten accesos directos a estos tipos de datos personales desde redes de terceros, Internet o redes inalámbricas.

B.1 Medidas de seguridad

Se han definido listas de controles y patrones de control que agrupan medidas de seguridad basadas principalmente en ISO/IEC 27002. La selección de medidas será de acuerdo con el nivel de riesgo obtenido y será conforme a las tablas de control definidas.

- Listas de controles. Utilizaremos este término para describir la situación en la que no es imperante implantar todos los controles sugeridos, sino que existirán medidas necesarias y medidas opcionales para que el responsable de seguridad seleccione aquéllas que, sumadas, apoyan a la mitigación del riesgo existente en el contexto de su organización. Es decir, en el caso de las listas la suma de controles contribuye a la protección de la información, teniendo la posibilidad de seleccionar uno a más controles. Existen listas de controles administrativos, de seguridad física y del entorno de red interna.

- Patrones de control. Utilizaremos este término para describir la situación en la que, de acuerdo a la situación de riesgo identificada, es necesario implantar en su totalidad los controles descritos dentro del mismo. Los patrones de control existentes son: Controles Básicos, DMZ y Caja Fuerte (entorno recomendado para resguardar información con nivel de riesgo por tipo de dato 4 y 5). Sólo se podrá descartar alguna medida de seguridad en el caso de que no sea aplicable a su infraestructura, por ejemplo un control enfocado a comercio electrónico se podrá descartar sólo si la organización no cuenta con dicha actividad.

B.2 Listas de medidas de seguridad

El responsable de seguridad deberá determinar el mínimo de controles opcionales que requiere conforme al contexto de su red.

Se cuenta con tres tipos de listas, cada una de ellas aplica para diferentes combinaciones de riesgo:

- AD: Lista de medidas administrativas, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista.
    a. AD-2. Medidas administrativas para nivel de riesgo por tipo de dato 2
    b. AD-3. Medidas administrativas para nivel de riesgo por tipo de dato 3
    c. AD-4-5. Medidas administrativas para nivel de riesgo por tipo de dato 4 o 5

- RI: Lista de medidas de seguridad aplicable para accesos desde la red interna, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse en la red.
    a. RI 1. Medidas básicas de seguridad para accesos desde red interna
    b. RI 2. Medidas intermedias de seguridad para accesos desde red interna
    c. RI 3. Medidas reforzadas de seguridad para accesos desde red interna

- F: Lista de medidas de seguridad aplicable para accesos desde el entorno físico, esta lista contiene controles mínimos necesarios y controles que de forma opcional el responsable de seguridad puede seleccionar para implantar en su organización. Se cuenta con tres niveles para esta lista; se debe considerar que la suma de controles contribuye a la disminución del riesgo que puede presentarse al acceder de forma física a los datos personales.
    a. FI 1. Medidas básicas de seguridad para accesos físicos
    b. FI 2. Medidas intermedias de seguridad para accesos físicos
    c. FI 3. Medidas reforzadas de seguridad para accesos físicos

B.2.1 Medidas administrativas

AD-2 Lista de medidas administrativas para nivel 2

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 2.

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual	6.1.5	Necesario
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene, procese, transmita u otorgue acceso datos personales o sensibles.	7.1.1	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser firmados por los empleados, contratistas y usuarios de terceros.	8.1.1	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo con lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad.	6.2.3	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales.	10.2.2	Opcional
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Realizar revisiones aleatorias de las bitácoras de acceso para identificar accesos no autorizados. Considerar una frecuencia semestral.	10.10.2	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Opcional

Lista AD-2			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Opcional

AD-3 Lista de medidas administrativas para nivel 3

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 3.

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	Necesario
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad	6.2.3	Necesario
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene, procese, transmita u otorgue acceso datos personales o sensibles.	7.1.1	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante.	8.1.1	Necesario
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Ninguno	8.1.3	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Mantener un procedimiento de monitoreo constante.	10.10.2	Necesario
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Necesario

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Necesario
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Proceso de autorización de instalaciones de procesamiento de la información: Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información debe ser definido e implementado.	Ninguno	6.1.4	Opcional
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión anual. Evitar conflictos de interés, puede ser revisión externa.	6.1.8	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Retorno de los activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.	Cotejar contra inventario los activos entregados al empleado, contratista o tercero.	8.3.2	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales pactadas contractualmente.	10.2.2	Opcional
Gestión de cambios a los servicios de terceros: Los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de políticas de seguridad, procedimientos y controles deberán ser gestionados. Considerando la criticidad de los sistemas de negocio, los procesos involucrados y la reevaluación de riesgos.	Se deberá incluir la autorización del responsable de seguridad en cualquier cambio que se realice en contratos o acuerdos de nivel de servicio con tercero.	10.2.3	Opcional
Aceptación del sistema: Se deberán establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones; se deberán llevar a cabo pruebas de los sistemas durante y previo a la aceptación de los mismos.	Ninguno	10.3.2	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de manejo de información: Se deberán documentar e implementar procedimientos para el manejo y almacenaje de información para protegerla de divulgación o uso no autorizado.	Documentar y autorizar las extracciones o transferencias de datos personales.	10.7.3	Opcional
Seguridad de la documentación de los sistemas: Deberá protegerse la documentación del sistema contra accesos no autorizados.	Definir un repositorio único para toda la documentación del sistema. Proteger el repositorio con contraseña. Cifrado Opcional.	10.7.4	Opcional
Política de control de acceso: Se deberá establecer, documentar y revisar una política de control de accesos. La misma deberá ser revisada de acuerdo a los requerimientos de negocio para los accesos.	Incluir: - Criterios para la generación y asignación de accesos - Responsabilidades del usuario Revisión anual de la política.	11.1.1	Opcional
Revisión de los derechos de acceso de usuario: La gerencia deberá revisar los derechos de acceso de los usuarios. Realizar estas revisiones en intervalos planeados, mediante un proceso formal.	Revisiones anuales	11.2.4	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional

Lista AD-3			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Reporte de vulnerabilidades de seguridad: Se debe requerir a todos los empleados, contratistas y terceras partes que notifiquen cualquier vulnerabilidad o evento de seguridad de la información en los sistemas o servicios.	Ninguno	13.1.2	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional

AD-4-5 Lista de medidas administrativas para nivel 4 y 5

A continuación se incluyen las medidas de seguridad administrativas aplicables a particulares con bases de datos personales con nivel de riesgo por tipo de dato 4 y 5.

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles por patrón como política de seguridad.	5.1.1	Necesario
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	Necesario
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	Necesario
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión semestral. Evitar conflictos de interés, puede ser revisión externa.	6.1.8	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Atender las necesidades de seguridad cuando se trata con clientes: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los clientes, a los activos o información de la organización.	Se deben identificar todas las interacciones entre la organización y el cliente en los cuales se involucren datos personales. Deberán tratarse como ejercicio de Derechos ARCO con una autenticación previa.	6.2.2	Necesario
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	El acuerdo debe estipular que el tercero conoce y se apega a la política de seguridad.	6.2.3	Necesario
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Documentar roles y responsabilidades en perfiles de puesto.	8.1.1	Necesario
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes, deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Ninguno	8.1.3	Necesario
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Ninguno	8.2.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Separación de funciones: Funciones y áreas de responsabilidad deben ser separados para reducir las oportunidades de modificación no autorizada o accidental, o mal uso de los activos de la organización.	Ninguno	10.1.3	Necesario
Aceptación del sistema: Se deberán establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones; se deberán llevar a cabo pruebas de los sistemas durante y previo a la aceptación de los mismos.	Ninguno	10.3.2	Necesario
Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.	Evitar el uso de medios removibles, cuando sea necesario justificar, documentar y autorizar su uso. Todos los medios removibles deberán ser inventariados como activos de información.	10.7.1	Necesario
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	Necesario
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Mantener un procedimiento de monitoreo constante.	10.10.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Política de control de acceso: Se deberá establecer, documentar y revisar una política de control de accesos. La misma deberá ser revisada de acuerdo a los requerimientos de negocio para los accesos.	Incluir: - Criterios para la generación y asignación de accesos - Responsabilidades del usuario Revisión anual de la política.	11.1.1	Necesario
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	Necesario
Administración de contraseñas de usuarios: La asignación de contraseñas deberá controlarse mediante un proceso formal de administración.	Gestión de cuentas privilegiadas.	11.2.3	Necesario
Revisión de los derechos de acceso de usuario: La gerencia deberá revisar los derechos de acceso de los usuarios. Realizar estas revisiones en intervalos planeados, mediante un proceso formal.	Revisiones anuales.	11.2.4	Necesario
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1	Necesario
Administración de llaves de cifrado: Se deben implantar procesos de administración de llaves de cifrado que soporten el uso de técnicas de cifrado en la organización.	Ninguno	12.3.2	Necesario

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	Considerar la aprobación del cambio por parte del responsable de seguridad. El procedimiento debe considerar la capacidad de realizar roll-back del cambio.	12.5.1	Necesario
Procedimientos y responsabilidades de respuesta a incidentes de seguridad de la información: Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad.	Incluir los criterios de tipificación de un incidente.	13.2.1	Necesario
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	Necesario
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno	6.1.3	Opcional
Proceso de autorización de instalaciones de procesamiento de la información: Un proceso de autorización de la administración para las nuevas instalaciones de procesamiento de información debe ser definido e implementado.	Ninguno	6.1.4	Opcional
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Investigación de antecedentes: Las verificaciones de antecedentes para todos los candidatos, contratistas y usuarios de terceras partes, deben llevarse a cabo de acuerdo a leyes relevantes, regulaciones y ética, y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información que será accedida y a los riesgos percibidos.	La investigación deberá ser proporcional a las responsabilidades del puesto.	8.1.2	Opcional
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	Opcional
Retorno de los activos: Todos los empleados, contratistas y usuarios de terceras partes, deben regresar a la organización todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.	Cotejar contra inventario los activos entregados al empleado, contratista o tercero.	8.3.2	Opcional
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	Opcional
Trabajando en áreas seguras: Se deberán diseñar y aplicar pautas y controles de protección física para trabajar en áreas seguras.	Considerar: - No ingresar a áreas seguras con dispositivos de almacenamiento móvil - No ingresar a áreas seguras con dispositivos de grabación de imágenes o video	9.1.5	Opcional
Seguimiento y revisión de los servicios de terceros: Los servicios, reportes y registros provistos por una tercera parte deberán ser monitoreados y revisados regularmente. Se deberán ejecutar auditorías de estos elementos de manera periódica.	Revisiones anuales pactadas contractualmente.	10.2.2	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Gestión de cambios a los servicios de terceros: Los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de políticas de seguridad, procedimientos y controles deberán ser gestionados. Considerando la criticidad de los sistemas de negocio, los procesos involucrados y la reevaluación de riesgos.	Se deberá incluir la autorización del responsable de seguridad en cualquier cambio que se realice en contratos o acuerdos de nivel de servicio con tercero.	10.2.3	Opcional
Procedimientos de manejo de información: Se deberán documentar e implementar procedimientos para el manejo y almacenaje de información para protegerla de divulgación o uso no autorizado.	Documentar y autorizar las extracciones o transferencias de datos personales, considerar cifrado de los datos para estas acciones.	10.7.3	Opcional
Seguridad de la documentación de los sistemas: Deberá protegerse la documentación del sistema contra accesos no autorizados.	Definir un repositorio único para toda la documentación del sistema. Proteger el repositorio con contraseña. Cifrado obligatorio.	10.7.4	Opcional
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno	11.3.3	Opcional
Análisis y especificación de los requerimientos de seguridad: Los requerimientos de nuevos sistemas o de mantenimientos de sistemas existentes deben especificar los controles de seguridad requeridos.	Debe existir una documentación de los requerimientos de seguridad para instalaciones, desarrollos y mantenimientos.	12.1.1	Opcional

Lista AD-4-5			
Control	**Parámetro**	**ID**	**Carácter**
Revisión técnica de aplicaciones después de cambios del sistema operativo: Cuando se cambian los sistemas operativos, aplicaciones críticas de negocio debe ser revisado y probado para asegurar que no hay impacto adverso en las operaciones de la organización o de seguridad.	La revisión de las condiciones de seguridad de la información debe ser realizada por personal de seguridad.	12.5.2	Opcional
Reporte de eventos de seguridad de la información: Se deben comunicar los eventos de seguridad de la información tan pronto como sea posible y de acuerdo a los canales de comunicación adecuados.	Ninguno	13.1.1	Opcional
Reporte de vulnerabilidades de seguridad: Se debe requerir a todos los empleados, contratistas y terceras partes que notifiquen cualquier vulnerabilidad o evento de seguridad de la información en los sistemas o servicios.	Ninguno	13.1.2	Opcional
Aprendizaje de los incidentes de seguridad: Se deben implantar los mecanismos necesarios para monitorear y cuantificar los costos y esfuerzos de los incidentes de seguridad de la información.	Documentar una base de conocimiento.	13.2.2	Opcional
Colección de evidencias: Cuando a raíz de un incidente de seguridad de la información se requieran acciones legales y acciones de seguimiento contra una persona o empresa, se deben recolectar, retener y presentar evidencias de acuerdo a las reglas de la jurisdicción.	Ninguno	13.2.3	Opcional

B.2.2 Medidas de seguridad de red interna

RI-1. Medidas básicas de seguridad para accesos desde red interna

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde la red interna.

Lista RI-1			
Control	**Parámetro**	**ID**	**Carácter**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso y usuario que accede.	10.10.1	Necesario
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Opcional

Lista RI-1			
Control	**Parámetro**	**ID**	**Carácter**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Opcional
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Frecuencia de verificación semestral	12.6.1	Opcional
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Opcional

RI-2. Medidas intermedias de seguridad para accesos desde red interna

A continuación se incluyen las medidas intermedias de seguridad para accesos a los datos personales desde la red interna.

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario y cambios a realizar Asegurar que se registren las actividades de administración del sistema	10.10.1 10.10.4	Necesario
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Poner especial atención en los usuarios de altos privilegios.	11.2.2	Necesario

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña de mínimo 10 caracteres	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2	Necesario
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1	Necesario
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Ninguno	9.2.6	Opcional
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2	Opcional

Lista RI-2			
Control	**Parámetro**	**ID**	**Carácter**
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4	Opcional
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Opcional
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP	10.10.6	Opcional
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo. En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Opcional

RI-3. Medidas avanzadas de seguridad para accesos desde red interna

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde la red interna.

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Ninguno	9.2.6	Necesario
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1	Necesario
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Eliminar contraseñas de fábrica Evitar protocolos de comunicación en texto claro	10.6.1	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario y cambios a realizar. Asegurar que se registren las actividades de administración del sistema.	10.10.1 10.10.4	Necesario

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	Poner especial atención en los usuarios de altos privilegios. Gestionar de forma centralizada los privilegios para reducir número de lugares donde se autentican y autorizan los accesos.	11.2.2	Necesario
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas	Contraseña de mínimo 12 caracteres	11.3.1	Necesario
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear	11.3.2	Necesario
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	No utilizar usuarios genéricos No compartir usuarios	11.5.2	Necesario
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1	Necesario

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo. En particular en los equipos que intervienen en el tratamiento de datos personales	12.3.1	Necesario
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1	Necesario
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2	Opcional
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4	Opcional
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Asegurar que los registros de auditoría no puedan modificarse	10.10.3	Opcional
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP	10.10.6	Opcional

Lista RI-3			
Control	**Parámetro**	**ID**	**Carácter**
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on)	Ninguno	11.5.1	Opcional
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 10 minutos como máximo para accesos a información personal	11.5.5	Opcional
Protección de las herramientas de auditoría de los sistemas de información: Se debe prevenir el acceso a las herramientas de auditoría de los sistemas de información para prevenir cualquier compromiso o mal uso de dicha información.	Cuando accedan a información personal	15.3.2	Opcional
Filtros de contenido para correo electrónico, internet y mensajería.	En particular cuidar las salidas de información personal	SM.1	Opcional

B.2.3 Medidas de seguridad de acceso físico

F-1. Medidas básicas de seguridad para accesos físicos

A continuación se incluyen las medidas básicas de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-1			
Control	**Parámetro**	**ID**	**Carácter**
Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados y llaves en archiveros y habitaciones que resguarden datos personales.	9.1.1	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Acceso Físico: Registrar fecha de acceso y usuario que accede.	10.10.1	Necesario
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional

Lista F-1			
Control	**Parámetro**	**ID**	**Carácter**
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.	9.2.5	Opcional
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	Opcional

F-2. Medidas intermedias de seguridad para accesos físicos

A continuación se incluyen las medidas intermedias de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Ninguno	8.3.3	Necesario
Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados, llaves y tarjetas de acceso en archiveros y habitaciones que resguarden datos personales.	9.1.1	Necesario
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7	Necesario
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	Necesario

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, nombre completo de la persona que accede y cambios a realizar	10.10.1	Necesario
Implementar un sistema de cámaras de seguridad.	Ninguno	SM.22	Necesario
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Considerar sitios donde se le de tratamiento a información física y electrónica. Considerar tarjetas de proximidad, teclados de combinación.	9.1.2	Opcional
Áreas de acceso público, carga y entrega: Los puntos de acceso tales como los de entrega, áreas de carga y otros puntos donde personas no autorizadas pueden entrar a las instalaciones, debe estar controladas y, si es posible, aisladas de las instalaciones donde se procesa información para evitar accesos no autorizados.	Ninguno	9.1.6	Opcional
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional

Lista F-2			
Control	**Parámetro**	**ID**	**Carácter**
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos, utilizar candados para equipos.	9.2.5	Opcional
Separación de la información en diferentes bases de datos e infraestructura.	Ninguno	SM.3	Opcional

F-3. Medidas reforzadas de seguridad para accesos físicos

A continuación se incluyen las medidas reforzadas de seguridad para accesos a los datos personales desde el entorno físico.

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Ninguno	8.3.3	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Considerar sitios donde se le de tratamiento a información física y electrónica. Considerar tarjetas de proximidad, biométricos, dobles factores de autenticación.	9.1.2	Necesario
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7	Necesario

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos (empulpado, trituración, incineración).	10.7.2	Necesario
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno	10.8.3	Necesario
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha y hora de acceso, nombre completo de la persona que accede, cambios a realizar y justificación de los cambios.	10.10.1	Necesario
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Proteger las bitácoras de acceso para evitar modificación o accesos no autorizados. Proteger los videos de vigilancia generados. Considerar controles de restricción física como se establece en 9.1.2 y 9.2.1	10.10.3	Necesario

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	Cada solicitud de acceso a los datos sensibles debe ser autorizada por el área de seguridad de la información.	11.2.2	Necesario
Implementar un sistema de cámaras de seguridad.	Ninguno	SM.22	Necesario
Monitorear cámaras de seguridad, respaldar y resguardar videos generados.	Resguardar respaldos durante un año.	SM.23	Necesario
Áreas de acceso público, carga y entrega: Los puntos de acceso tales como los de entrega, áreas de carga y otros puntos donde personas no autorizadas pueden entrar a las instalaciones, debe estar controladas y, si es posible, aisladas de las instalaciones donde se procesa información para evitar accesos no autorizados.	Ninguno	9.1.6	Opcional
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno	9.2.1	Opcional
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos, utilizar candados, alarmas y mensajes grabados físicamente en el equipo.	9.2.5	Opcional
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4	Opcional

Lista F-3			
Control	**Parámetro**	**ID**	**Carácter**
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Evitar el acceso a áreas seguras con artículos o accesorios que permitan la extracción de información personal. Revisiones físicas a la salida de las personas para detectar posibles fugas de información personal.	12.5.4	Opcional
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno	SM.2	Opcional
Separación de la información en diferentes bases de datos e infraestructura	Ninguno	SM.3	Opcional

B.3 Patrones de control

Se han definido dos tipos de patrones, cada uno de ellos con niveles de patrón que atienden a diferentes combinaciones de riesgo. A continuación se listan:

- CB: Patrón de control de medidas de seguridad básicas, es aplicable para aquellos particulares cuyo nivel de riesgo por tipo de dato es igual a 1.

- DMZ: Patrón para accesos desde entornos de alta anonimidad, hace referencia a la necesidad de implementar una zona desmilitarizada como zona de transición entre un entorno de mayor riesgo y uno de menor riesgo. Se contemplan tres niveles de este patrón.
    a. DMZ 2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad
    b. DMZ 3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad

- CF: Patrón aplicable para datos de nivel 4 y 5 de riesgo por tipo de dato, su nombre hace referencia las iniciales de Caja Fuerte, debido a que se recomienda que estos tipos de datos se protejan con medidas de seguridad mucho más estrictas y se construya una caja fuerte alrededor de ellos para protegerlos de accesos no autorizados. Se contemplan dos niveles para este patrón. Cabe mencionar que una vez implementada la caja fuerte, el acceso a ella y salida de información de esta debe controlarse estrictamente.
    a. CF 1. Patrón de control de medidas de seguridad para caja fuerte nivel 1
    b. CF 2. Patrón de control de medidas de seguridad para caja fuerte nivel 2

B.3.1 Medidas de seguridad básicas

Con el objetivo de simplificar la operación y administración de las medidas de seguridad para el nivel de riesgo “1” se recomienda la documentación e implementación de un Contrato de Adhesión (CDA), que conjunte de forma sencilla los controles y funja con una lista de control de accesos a los datos personales.

El CDA deben incluir los accesos permitidos a los datos personales, el inventario de bases de datos físicas y electrónicas, así como las medidas de seguridad implementadas. Todos los empleados que intervengan en el tratamiento de datos personales deberán firmarlo.

El Contrato de Adhesión (CDA) puede ser consultado en el ANEXO A.

CB. Patrón de control de medidas de seguridad básicas

A continuación se listan las medidas de seguridad básicas y un mapeo con el contrato de adhesión (CDA).

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por la alta gerencia, publicada y comunicada a todos los empleados y terceras partes relevantes.	Considerar la lista de controles como política de seguridad.	5.1.1	1
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Revisión anual o cuando exista una modificación a las medidas o procesos de seguridad, o las condiciones de riesgo.	5.1.2	1
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Ninguno.	6.1.3	1
Acuerdos de confidencialidad: Los requisitos para los acuerdos de confidencialidad o de no revelación deben reflejar las necesidades de protección de información de la organización y deben ser revisados periódicamente.	Revisión anual.	6.1.5	1.1
Revisión independiente de la seguridad de la información: El enfoque de la organización hacia el manejo de la seguridad de la información y su implementación (por ejemplo, objetivos de control, controles, políticas, procesos y procedimientos para seguridad) debe ser revisado de manera independiente en intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.	Revisión anual del documento de autoevaluación o el Contrato de Adhesión (CDA).	6.1.8	2

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Abordar la seguridad en los acuerdos de terceros: Los acuerdos con terceros deben cubrir todos los requisitos de seguridad pertinentes, cuando estén relacionados con el acceso, tratamiento, comunicación o gestión de la información o de las instalaciones de procesamiento de información de la organización, o la adición de productos o servicios a las instalaciones de procesamiento de la información.	Los terceros que accedan a los datos deben firmar la lista de accesos de personal autorizado, indicando la actividad a realizar, fecha o rango de fechas en las que tendrán acceso y aceptar el conocimiento de las medidas de seguridad necesarias para la protección de los datos personales.	6.2.3	1
Inventario de activos: Todos los activos deben ser claramente identificados y un inventario de los activos más importantes deber ser elaborado y mantenido.	Considerar dentro del inventario cualquier activo físico o lógico que almacene o procese datos personales o sensibles.	7.1.1	3.1
Uso aceptable de los activos: Deben identificarse, documentarse e implementarse reglas para el uso aceptable de la información y los activos relacionados con las instalaciones de procesamiento de información.	Evitar cualquier actividad que comprometa los datos personales para protegerlos de divulgación o uso no autorizado.	7.1.3	1.1
Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceras partes, deben estar definidos y documentados en concordancia con la política de seguridad de la información de la organización.	Agregar roles y responsabilidades de protección de datos dentro de todo contrato vinculante. Estos contratos deben ser firmados por los empleados, contratistas y usuarios de terceros.	8.1.1	1.2

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la organización y, cuando sea relevante, contratistas y usuarios de terceras partes, deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.	Sólo considerar campañas anuales de concienciación.	8.2.2	1.1
Proceso disciplinario: Debe existir un proceso disciplinario formal para aquellos empleados que han cometido una brecha de seguridad.	Ninguno	8.2.3	1.3
Eliminación de los derechos de acceso: Los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes, a información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Cotejar contra inventario los accesos y cuentas entregadas al empleado, contratista o tercero.	8.3.3	3.1
Controles físicos de entrada: Las áreas seguras deben estar protegidas con controles de entrada para asegurar que únicamente personal autorizado tenga permitido el acceso.	Restringir el acceso a la información en soporte físico a través de mecanismos de acceso como candados y llaves en archiveros y habitaciones que resguarden datos personales.	9.1.2	3
Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	Ninguno.	9.2.1	3.2
Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.	Actuar conscientemente para prevenir el posible robo o acceso no autorizado a los equipos.	9.2.5	1.1

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno.	10.4.1	3
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Considerar contraseñas para los dispositivos de red diferentes a las provistas por defecto. WIFI: establecer contraseña.	10.6.1	3
Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.	Cuando el tratamiento de la información ya no sea necesario. Garantizar la destrucción de los medios físicos que contengan datos personales y sensibles de tal forma que no sea posible reconstruirlos.	10.7.2	4
Acuerdos de intercambio de información: Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre la organización y entidades externas.	Considerar los acuerdos de intercambio de información dentro del aviso de privacidad de la organización y los contratos vinculantes con el receptor de la información, de acuerdo a lo establecido en la LFPDPPP y su Reglamento.	10.8.2	1.1
Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la organización.	Ninguno.	10.8.3	1.1

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Registrar las personas con acceso autorizado a los datos personales incluyendo fecha de acceso (o rango de acceso permitido) y firma.	10.10.1	1
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Validar, y documentar las altas de accesos. Garantizar la revocación de accesos inmediatamente después a una baja. Generar inventario que considere todos los accesos entregados a toda persona.	11.2.1	3
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña.	11.3.1	3
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2	3
Política de escritorios y pantallas limpias: Se deberá implementar una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	Ninguno.	11.3.3	1
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Instalación de actualizaciones semestralmente.	12.6.1	3

Patrón de control CB			
Control	**Parámetro**	**ID**	**CDA**
Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	Revisiones anuales, considerando como estándares de seguridad los controles de esta lista.	15.2.2	2

B.3.2 Patrones de control para DMZ

DMZ-2. Patrón de control de medidas intermedias de seguridad para accesos desde entornos de alta anonimidad

A continuación se incluye la representación gráfica (Figura 7) del patrón de control para mitigar el riesgo cuando los accesos a los datos personales son desde redes inalámbricas, redes de terceros o internet; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

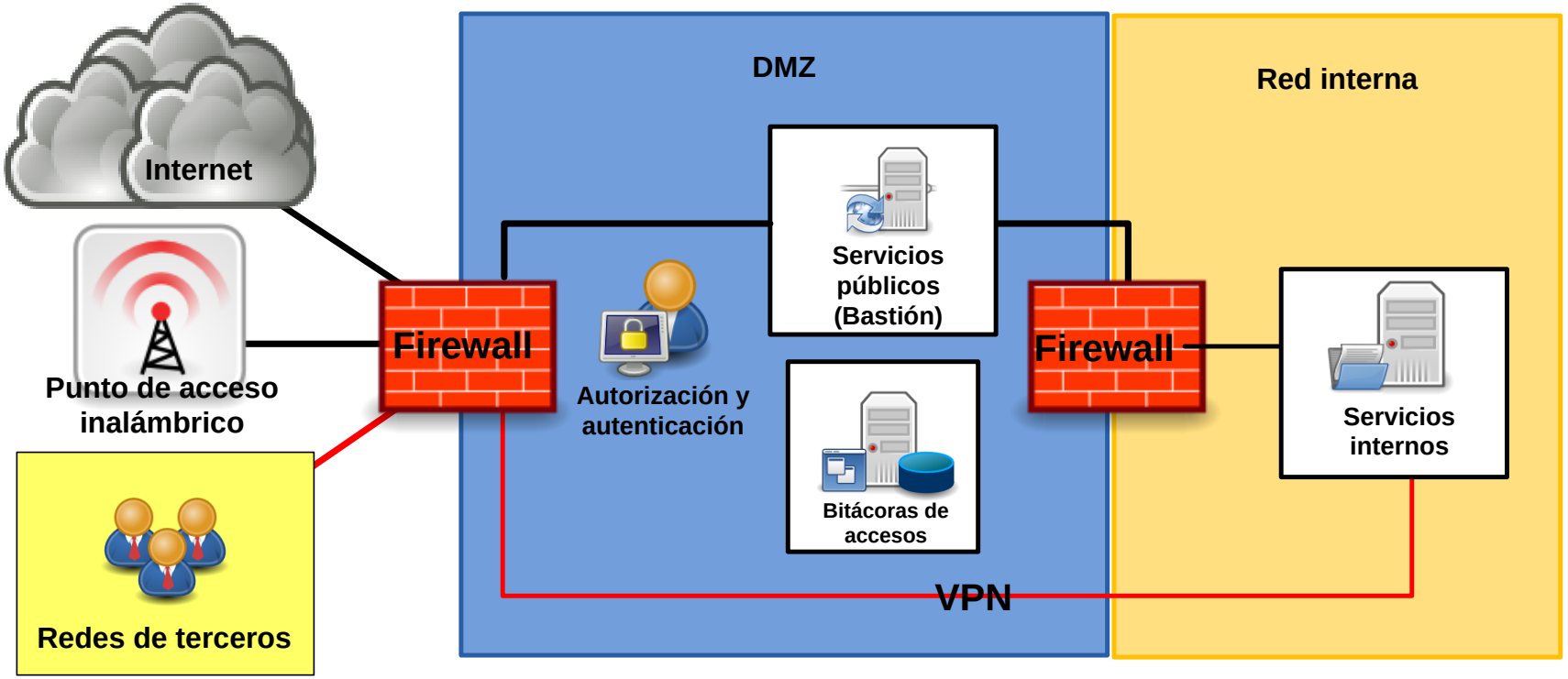

Figura 7. Patrón de control de DMZ-2

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Evitar uso de protocolos en texto claro Eliminar contraseñas por defecto	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Protocolos Seguros Cifrado del medio Autenticación Disociación de información cuando los datos pasen a un entorno de mayor anonimidad.	10.8.1
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar registrar los accesos a los datos personales y las salidas de información. Incluir IP origen e IP destino para cada conexión.	10.10.1
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	El área de seguridad debe estar involucrada en el proceso de autorización	11.2.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Ninguno	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde o hacia redes de terceros, red inalámbrica o internet, para tratar datos personales, debe ser por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo	12.3.1
Definir e implementar listas de control de acceso (ACL)	Ninguno	SM.29
Controles de DNS	Ninguno	SM.30
Únicamente permitir servicios públicos dentro de la DMZ	Ninguno	SM.31
Mejores prácticas de configuración del FW	Ninguno	SM.32
Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.33

Patrón de control DMZ-2		
Control	**Parámetro**	**ID**
Red de terceros conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.34
Controles de tráfico entrante y saliente	NO internet hacia LAN Si LAN hacia internet Si DMZ hacia LAN y desde Si Internet hacia y desde DMZ No permitir conexión desde el exterior hacia interior (sin pasar x DMZ)	SM.35

DMZ-3. Patrón de control de medidas reforzadas de seguridad para accesos desde entornos de alta anonimidad

A continuación se incluye la representación gráfica (Figura 8) del patrón de control para mitigar el riesgo cuando los accesos a los datos personales son desde redes inalámbricas, redes de terceros o internet; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

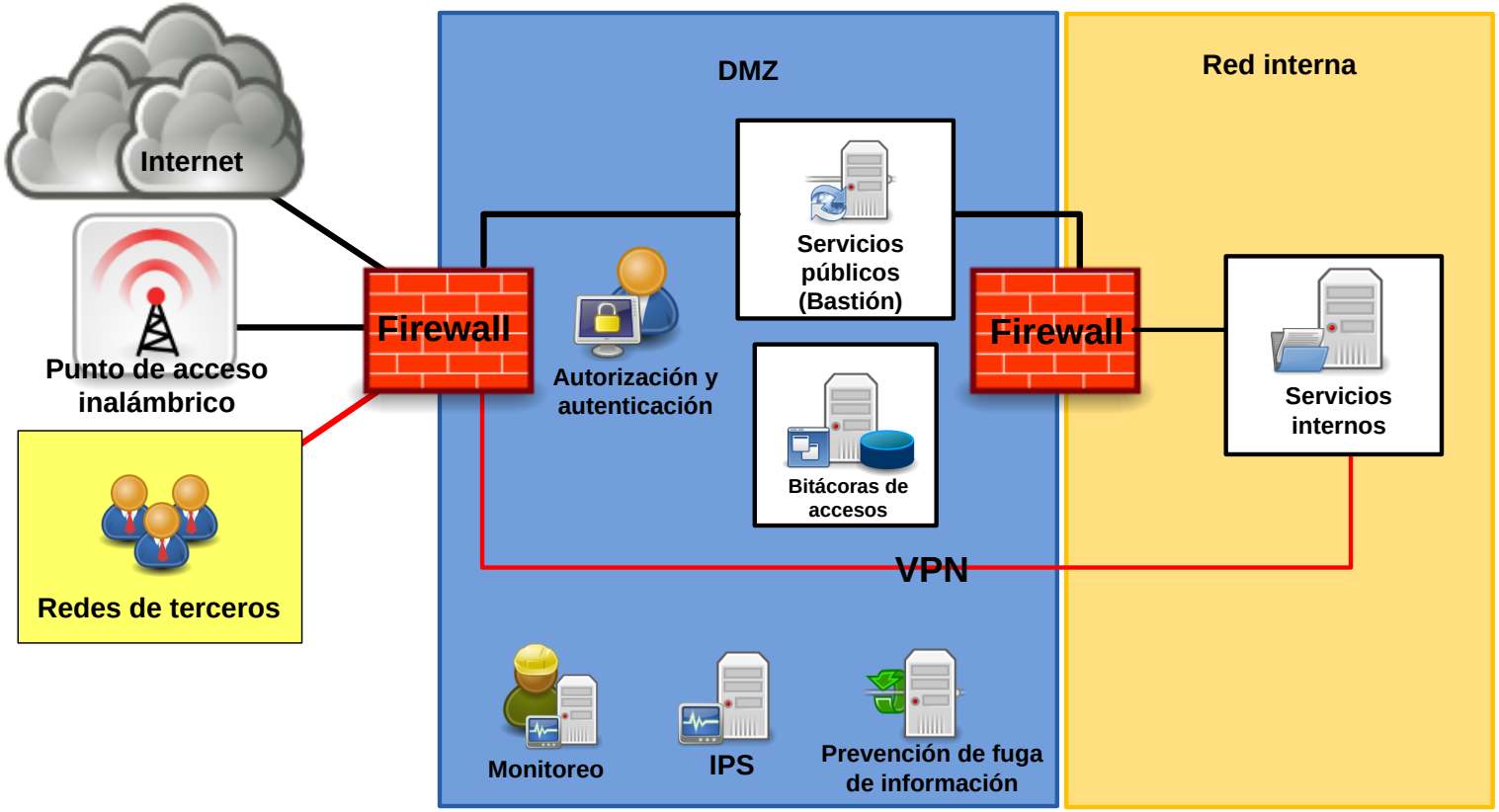

Figura 8. Patrón de control de DMZ-3

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Evitar uso de protocolos en texto claro Eliminar contraseñas por defecto	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Protocolos Seguros Cifrado del medio Autenticación Disociación de información cuando los datos pasen a un entorno de mayor anonimidad.	10.8.1
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar registrar los accesos a los datos personales y las salidas de información. Incluir IP origen e IP destino para cada conexión.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Establecer un sistema de monitoreo continuo de los accesos a los datos personales.	10.10.2
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios	El área de seguridad debe de estar involucrado en el proceso de autorización	11.2.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Ninguno	11.4.1

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	Ninguno	11.4.7
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Disociación de información cuando los datos pasen de un ambiente de riesgo menor a un ambiente de riesgo mayor.	Ninguno	SM.2
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo	12.3.1
Definir e implementar listas de control de acceso (ACL)	Ninguno	SM.29
Controles de DNS	Ninguno	SM.30

Patrón de control DMZ-3		
Control	**Parámetro**	**ID**
Únicamente permitir servicios públicos dentro de la DMZ	Ninguno	SM.31
Mejores prácticas de configuración del FW	Ninguno	SM.32
Red inalámbrica conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.33
Red de terceros conectada a la zona desmilitarizada (DMZ) externa	Ninguno	SM.34
Controles de tráfico entrante y saliente	NO internet hacia LAN Si LAN hacia internet Si DMZ hacia LAN y desde Si Internet hacia y desde DMZ No permitir conexión desde el exterior hacia interior (sin pasar x DMZ)	SM.35
Implementar y monitorear sistemas de prevención de Intrusos (IPS)	Ninguno	SM.36

B.3.3 Patrones de control para caja fuerte

CF-1. Patrón de control de medidas de seguridad para caja fuerte nivel 1

A continuación se incluye la representación gráfica (Figura 9) del patrón de control correspondiente a la caja fuerte; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

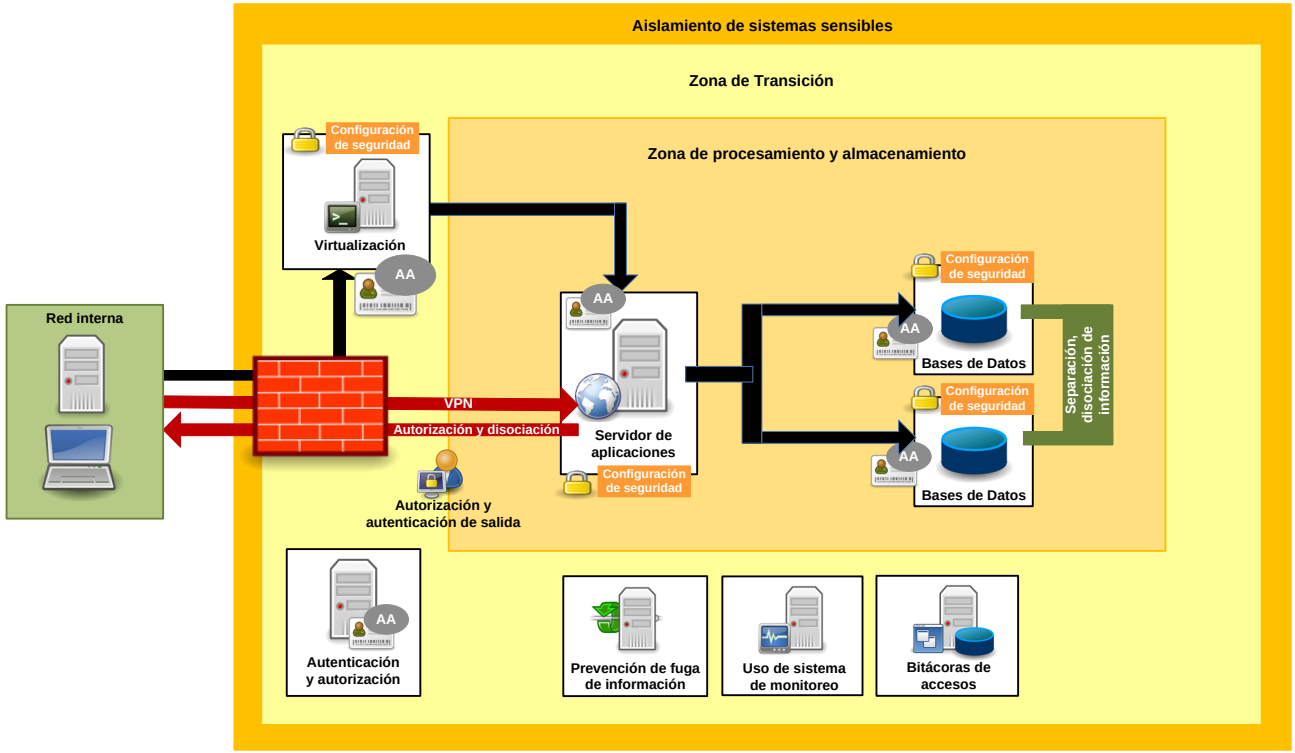

Figura 9. Patrón de control de CF-1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Ninguno	9.2.6
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Uso de protocolos seguros Eliminar contraseñas por defecto.	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Se requiere la existencia de una zona de transición en la caja fuerte para evitar que se tenga acceso de forma directa a los datos desde entornos ajenos a la caja fuerte. Considerar los siguientes controles: - Protocolos seguros. - Cifrado del medio. - Autenticación. -Disociación de información cuando los datos salgan de la caja fuerte.	10.8.1
Comercio electrónico: La información involucrada en el comercio electrónico que circule por redes públicas, deberá protegerse de la actividad fraudulenta, divulgación o modificación no autorizada.	Considerar cifrado de los datos ingresados en sitios de comercio electrónico, certificados de seguridad para la transacción.	10.9.1
Transacciones en línea: La información involucrada en transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración, divulgación, duplicación o reproducción no autorizada.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	10.9.2

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario, cambios realizados, equipo origen y destino. Asegurar que se registren las actividades de administración del sistema. Garantizar la generación de estas bitácoras.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Ninguno	10.10.2
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Ninguno	10.10.3
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP.	10.10.6
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Se debe considerar la autorización de acceso a los datos sensibles por el área de seguridad de la información en cada solicitud de acceso.	11.2.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	El área de seguridad debe estar involucrada en el proceso de autorización. Controlar de la cantidad de datos sensibles que puede tratar un usuario autorizado, con el objetivo de evitar que tenga contacto con una gran cantidad de datos o con las bases de datos completas, mediante el control de tablas y campos.	11.2.2
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña de mínimo 12 caracteres.	11.3.1
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde cualquier entorno diferente a la caja fuerte para tratar datos personales, debe ser a través de una zona de transición interna, evitando el acceso directo a los datos y por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Identificación de los equipos en la red: La identificación automática de equipo deberá considerarse como un medio de autenticación de conexiones desde lugares y equipos específicos.	Identificación del equipo por medio de dirección MAC o dirección IP.	11.4.3
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on).	Usar protocolos seguros de autenticación.	11.5.1
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2
Uso de utilidades del sistema: se debe restringir y controlar el uso de programas que tengan la capacidad de sobrepasar los controles de seguridad de los sistemas y de las aplicaciones.	Ninguno	11.5.4
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 5 minutos como máximo.	11.5.5

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Aislamiento de sistemas sensibles: los sistemas sensibles deben tener un entorno informático independiente y aislado.	Este control se ve reflejado en la implementación de la caja fuerte.	11.6.2
Validación de los datos de entrada: Se deben validar los datos de entrada a las aplicaciones para asegurar que los datos son apropiados y correctos.	Ninguno	12.2.1
Validación de los datos de salida: Se deben validar los datos de salida de las aplicaciones para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.	Ninguno	12.2.4
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1
Protección de los datos de prueba de los sistemas: Se debe seleccionar cuidadosamente los datos de prueba y deben ser controlados y protegidos adecuadamente.	Considerar la no utilización de datos de producción en ningún ambiente fuera del operativo.	12.4.2
Control de accesos al código fuente: Se debe restringir el acceso al código fuente de los programas.	Ninguno	12.4.3
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1

Patrón de control CF-1		
Control	**Parámetro**	**ID**
Separación de la información en diferentes bases de datos e infraestructura.	Separar la información en bases de datos de menor tamaño para disminuir el interés de un tercero. La separación implica que se implemente una autenticación diferente para cada base de datos.	SM.3
Virtualización de equipos y acceso a la información a través de clientes delgados que impidan guardar la información que se accede en el equipo del usuario.	Ninguno	SM.12
En caso de requerir visualizar o tratar datos personales por medio de sistemas de información o ambientes distintos a producción, se deberán establecer mecanismos de enmascaramiento para prevenir el mal uso de los datos personales y sensibles.	Ninguno	SM.20

CF-2. Patrón de control de medidas de seguridad para caja fuerte nivel 2

A continuación se incluye la representación gráfica (Figura 10) del patrón de control correspondiente a la caja fuerte; cabe mencionar que esta representación no incluye la totalidad de las medidas recomendadas. Para verificar el total de medidas de seguridad que forman parte del patrón, se debe ver la tabla posterior al gráfico.

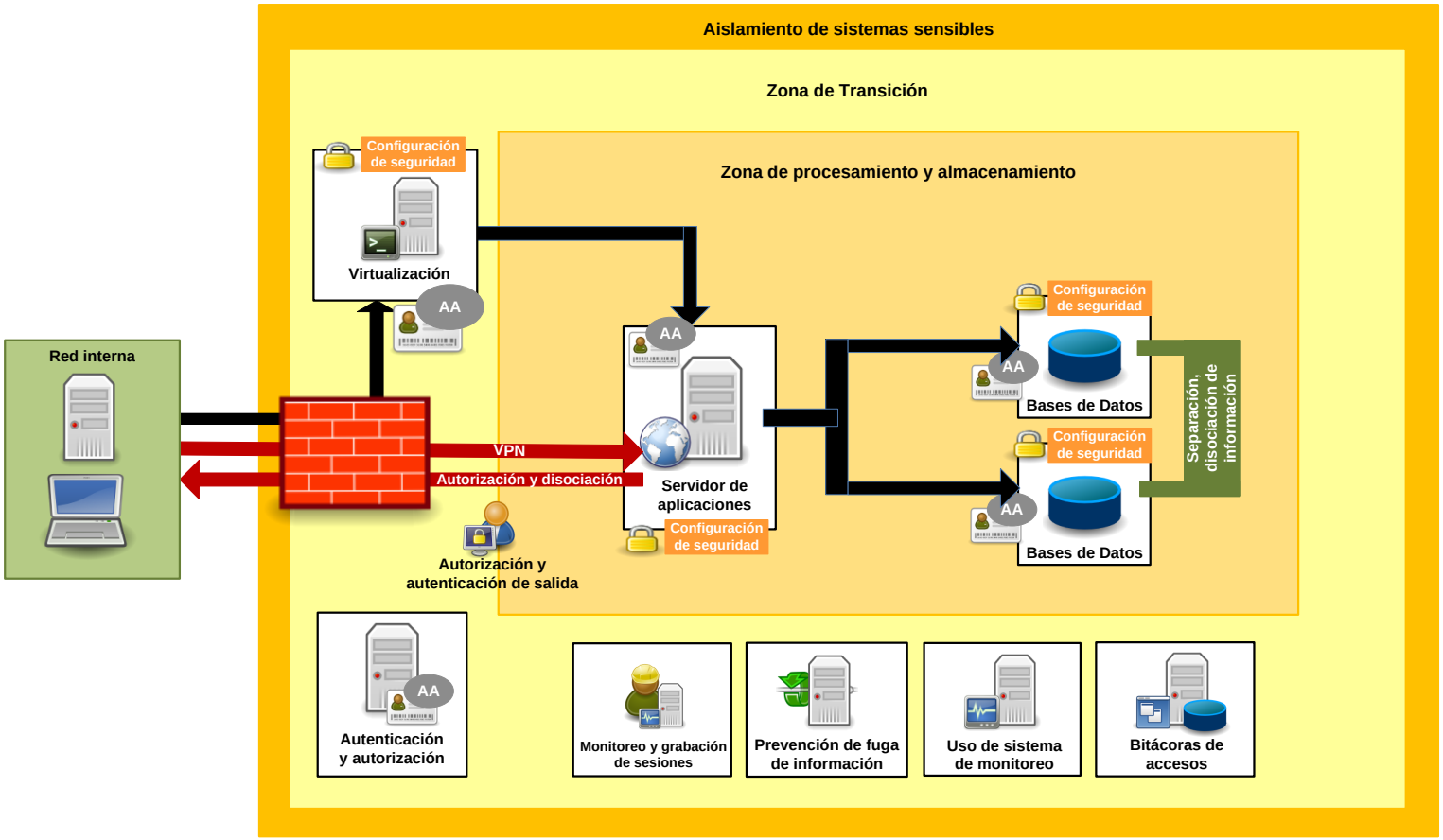

Figura 10. Patrón de control de CF-2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación.	Ninguno	9.2.6
Autorización de salida: No se sacará equipo, información o "software" fuera de las instalaciones sin previa autorización.	Ninguno	9.2.7
Gestión del cambio: Los cambios en las instalaciones de procesamiento y sistemas de información deben ser controlados.	Considerar la autorización del responsable de seguridad previo a cualquier cambio. Se recomienda alinear las prácticas de gestión del cambio a las propuestas de ITIL.	10.1.2
Separación de instalaciones de desarrollo, prueba y operaciones: Las instalaciones de desarrollo, prueba y operaciones deberán ser separadas para reducir los riesgos de acceso o cambios no autorizados a sistemas operacionales.	Ninguno	10.1.4
Controles contra código malicioso: Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Ninguno	10.4.1
Respaldos de información: Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.	Respaldo seguro de datos personales, garantizando que el respaldo tenga el mismo nivel de protección que la base de datos.	10.5.1

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	Uso de protocolos seguros Eliminar contraseñas por defecto.	10.6.1
Políticas y procedimientos de intercambio de información: Se deberán implementar políticas, procedimientos y controles formales de intercambio para proteger la información que transite a través de cualquier tipo de instalaciones de comunicaciones.	Se requiere la existencia de una zona de transición en la caja fuerte para evitar que se tenga acceso de forma directa a los datos desde entornos ajenos a la caja fuerte. Considerar los siguientes controles: - Protocolos seguros. - Cifrado del medio. - Autenticación. -Disociación de información cuando los datos salgan de la caja fuerte.	10.8.1
Comercio electrónico: La información involucrada en el comercio electrónico que circule por redes públicas, deberá protegerse de la actividad fraudulenta, divulgación o modificación no autorizada.	Considerar cifrado de los datos ingresados en sitios de comercio electrónico, certificados de seguridad para la transacción.	10.9.1
Transacciones en línea: La información involucrada en transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración, divulgación, duplicación o reproducción no autorizada.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	10.9.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	Considerar el registro de cualquier acceso desde cualquier entorno a datos personales y sensibles. Registrar fecha de acceso, usuario, cambios realizados, equipo origen y destino. Asegurar que se registren las actividades de administración del sistema. Garantizar la generación de estas bitácoras.	10.10.1
Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Ninguno	10.10.2
Protección de información de registros: Se deberán proteger las instalaciones e información de registro contra modificación y accesos no autorizados.	Ninguno	10.10.3
Sincronización de relojes: Se deberán sincronizar con una fuente común los relojes de todos los sistemas de procesamiento de información relevantes.	Utilizar protocolo NTP.	10.10.6
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Se debe considerar la autorización de acceso a los datos sensibles por el área de seguridad de la información en cada solicitud de acceso.	11.2.1

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.	El área de seguridad debe estar involucrada en el proceso de autorización. Controlar de la cantidad de datos sensibles que puede tratar un usuario autorizado, con el objetivo de evitar que tenga contacto con una gran cantidad de datos o con las bases de datos completas, mediante el control de tablas y campos.	11.2.2
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	Contraseña de mínimo 12 caracteres.	11.3.1
Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Considerar bloqueo automático del equipo a los 5 minutos con solicitud de contraseña para desbloquear.	11.3.2
Política de uso de los servicios de red: Los usuarios sólo deben contar con acceso a los servicios para los que han sido autorizados.	Bloquear o dar de baja puertos y servicios innecesarios en equipos de cómputo.	11.4.1
Autenticación del usuario para las conexiones externas: Se deberá utilizar métodos apropiados de autenticación para controlar el acceso de usuarios remotos.	La conexión a los sistemas de información desde cualquier entorno diferente a la caja fuerte para tratar datos personales, debe ser a través de una zona de transición interna, evitando el acceso directo a los datos y por medio de soluciones de red privada virtual que cuenten con métodos robustos de autenticación y cifrado.	11.4.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Identificación de los equipos en la red: La identificación automática de equipo deberá considerarse como un medio de autenticación de conexiones desde lugares y equipos específicos.	Identificación del equipo por medio de dirección MAC o dirección IP.	11.4.3
Protección de puertos para soporte y administración remota: Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.	Ninguno	11.4.4
Control de conexión de red: Se deberá restringir la capacidad de los usuarios para conectarse a redes compartidas de acuerdo a la política de control de acceso y los requisitos de las aplicaciones de negocio, poniendo especial énfasis en redes que se extiendan más allá de las fronteras de la organización.	Ninguno	11.4.6
Control de enrutamiento de la red: Los controles de enrutamiento deben aplicarse a las redes para garantizar que las conexiones informáticas y los flujos de información no violan la política de control de acceso de las aplicaciones de negocio.	Ninguno	11.4.7
Procedimientos de acceso seguro a los sistemas (log-on): Se debe controlar el acceso a los sistemas operativos, mediante un proceso seguro de inicio de sesión (log-on).	Usar protocolos seguros de autenticación.	11.5.1
Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Ninguno	11.5.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Uso de utilidades del sistema: se debe restringir y controlar el uso de programas que tengan la capacidad de sobrepasar los controles de seguridad de los sistemas y de las aplicaciones.	Ninguno	11.5.4
Tiempo de expiración de las sesiones: se deben desactivar las sesiones inactivas después de un periodo de inactividad definido.	Considerar como tiempo de expiración 5 minutos como máximo.	11.5.5
Límite del tiempo de conexión: se deben utilizar restricciones a los tiempos de conexión para proveer seguridad adicional para las aplicaciones de alto riesgo.	Ninguno	11.5.6
Aislamiento de sistemas sensibles: los sistemas sensibles deben tener un entorno informático independiente y aislado.	Este control se ve reflejado en la implementación de la caja fuerte.	11.6.2
Validación de los datos de entrada: Se deben validar los datos de entrada a las aplicaciones para asegurar que los datos son apropiados y correctos.	Ninguno	12.2.1
Integridad de los mensajes: Se deben definir e implantar los controles apropiados para asegurar la autenticidad de los mensajes y para proteger su integridad dentro de las aplicaciones.	Implementar controles de no repudio, considerando cifrado de los datos, certificados de seguridad.	12.2.3
Política sobre el uso de controles criptográficos: Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	Ninguno	12.3.1
Protección de los datos de prueba de los sistemas: Se debe seleccionar cuidadosamente los datos de prueba y deben ser controlados y protegidos adecuadamente.	Considerar la no utilización de datos de producción en ningún ambiente fuera del operativo.	12.4.2

Patrón de control CF-2		
Control	**Parámetro**	**ID**
Control de accesos al código fuente: Se debe restringir el acceso al código fuente de los programas.	Ninguno	12.4.3
Fuga de información: Se deben prevenir las oportunidades de fuga de información.	Ninguno	12.5.4
Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la organización a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Ninguno	12.6.1
Separación de la información en diferentes bases de datos e infraestructura.	Separar la información en bases de datos de menor tamaño para disminuir el interés de un tercero. La separación implica que se implemente una autenticación diferente para cada base de datos.	SM.3
Virtualización de equipos y acceso a la información a través de clientes delgados que impidan guardar la información que se accede en el equipo del usuario.	Ninguno	SM.12
En caso de requerir visualizar o tratar datos personales por medio de sistemas de información o ambientes distintos a producción, se deberán establecer mecanismos de enmascaramiento para prevenir el mal uso de los datos personales y sensibles.	Ninguno	SM.20
Monitoreo y grabación del tratamiento de la información sensible que realizan los usuarios.	Ninguno	SM.25