CIATEC

DOCUMENTO DE SEGURIDAD DEL CIATEC, A.C.

Introducción

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

El artículo 25 de la Ley señala que el responsable del tratamiento deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

El artículo 26 de la Ley, señala las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para las personas titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de personas titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Al respecto, el artículo 27 de la Ley, señala lo siguiente:

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

En el artículo 29 de la Ley establece como una obligación la elaboración de un documento de seguridad, que se define como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, deberá contener, como mínimo la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Objetivo

Instaurar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales biométricos (huella, imagen facial) del personal del CIATEC, A.C., en posesión de la Gerencia de Recursos Humanos y la Gerencia de Tecnologías de Información y Comunicaciones adscritas a la Dirección Administrativa, que permitan protegerlos, así como garantizar su confidencialidad, integridad y disponibilidad.

I. El inventario de datos personales y de los sistemas de tratamiento

Unidad Administrativa: Dirección Administrativa.

Áreas: Gerencia de Recursos Humanos y la Gerencia de Tecnologías de Información y Comunicaciones.

Finalidad: Concentrar la información de los datos personales biométricos (huella, imagen facial) del personal del CIATEC, A.C., de forma ordenada, segura, íntegra a través de medidas de seguridad de carácter administrativo, físico y técnico para su protección.

Inventario de datos personales

Nombre completo
Huella
Imagen facial
Número de empleado

II. Las funciones y obligaciones de las personas que traten datos personales

Medio por el que se obtiene el dato personal biométrico

Se realiza el registro de la información (nombre completo, huella, imagen facial, número de empleado) en el sistema "Hik Central Professional", por la persona de Servicios Personales, que pertenece al área de Recursos Humanos.

Responsable del sistema

Nombre: Gloria Margarita Rangel Armenta
Cargo: Gerente de Tecnologías de Información y Comunicaciones
Funciones: Establecer y supervisar las acciones de manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad, y exactitud de la información contenida en dichos sistemas.

Encargada del sistema

Nombre: Patricia Sánchez
Cargo: Gerente de Recursos Humanos
Funciones: Establecer y supervisar las acciones de manejo, mantenimiento, seguridad y protección de los sistemas de datos personales, así como de la integridad, confiabilidad, disponibilidad, y exactitud de la información contenida en dichos sistemas.

El Responsable del sistema, deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, como lo dispone el artículo 25 de la Ley.

De conformidad con el artículo 2 fracciones XIX, XX y XXI de la Ley, se establecen las siguientes medidas de seguridad:

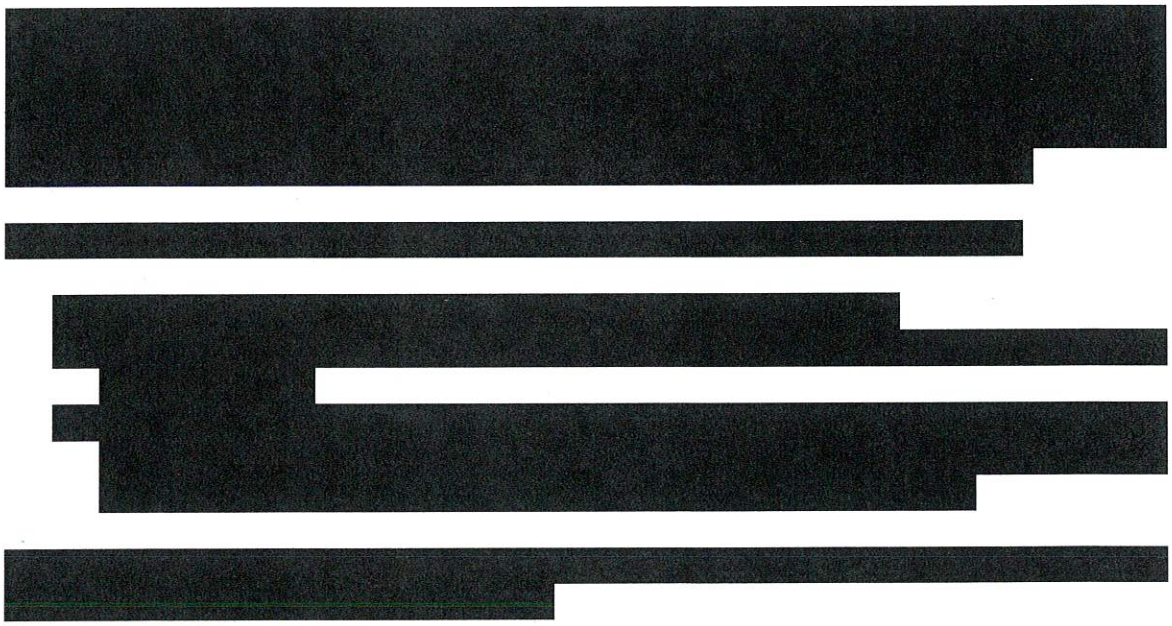
Medidas de seguridad administrativas: las áreas de Recursos Humanos y Tecnologías de Información y Comunicaciones, generan el presente documento de seguridad, el cual establece las acciones, medidas a seguir para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y eliminación de la información, así como la sensibilización y capacitación del personal, con la finalidad de garantizar el uso adecuado de los Datos Personales.

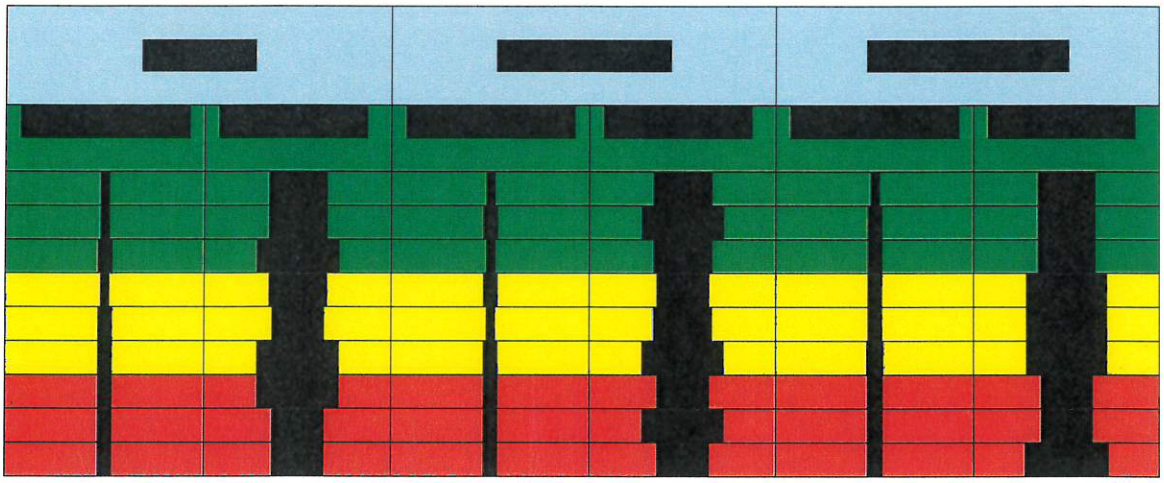
Medidas de seguridad físicas: CIATEC, cuenta con medidas de control para el acceso a las instalaciones, se tienen protocolos para el acceso a la institución a fin de prevenir el ingreso no autorizado a las instalaciones del CIATEC.

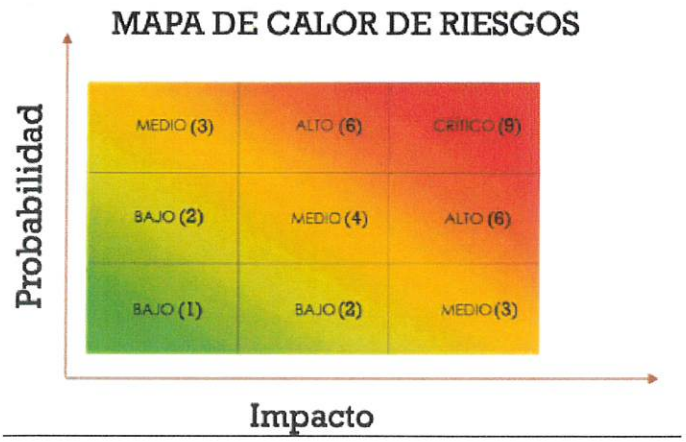
Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

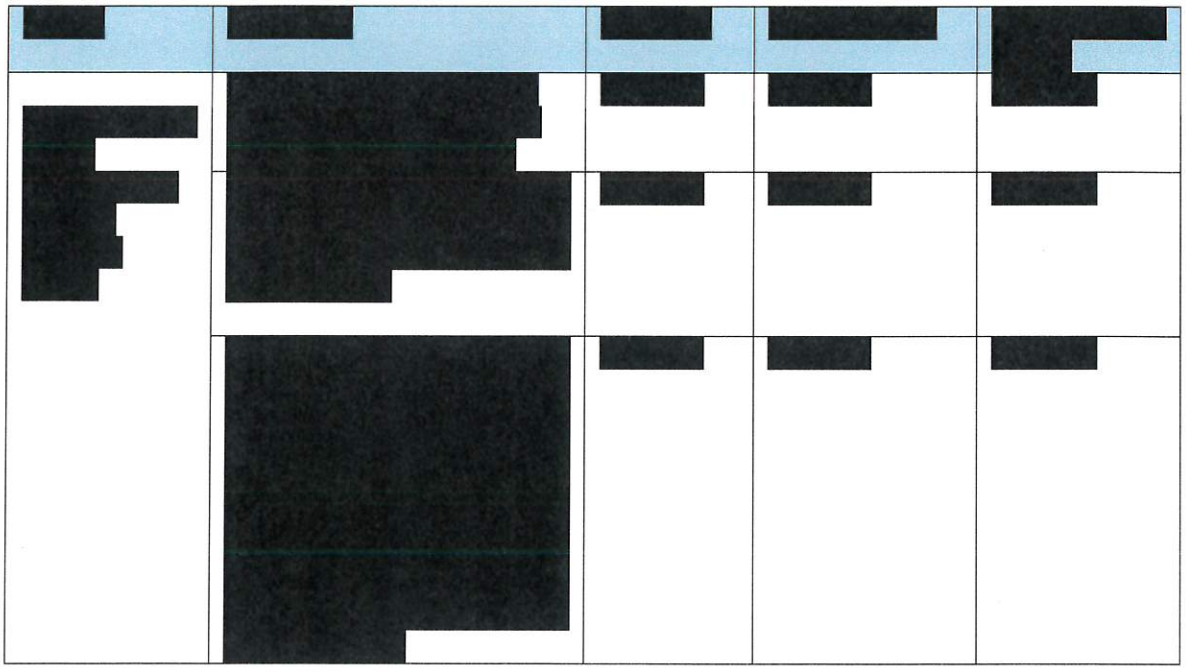
Los equipos de cómputo que se asignan a las áreas señaladas para el cumplimiento de sus funciones, así como los equipos destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los Sistemas de información cuentan con un programa de mantenimiento periódico en el que se ejecutan acciones preventivas y en su caso, correctivas con el objetivo de promover un mantenimiento eficaz y salvaguardar la información que hospedan.

III. Análisis de riesgo






MAPA DE CALOR DE RIESGOS
Probabilidad
MEDIO (3)
ALTO (6)
CRITICO (9)
BAJO (2)
MEDIO (4)
ALTO (6)
BAJO (1)
BAJO (2)
MEDIO (3)
Impacto

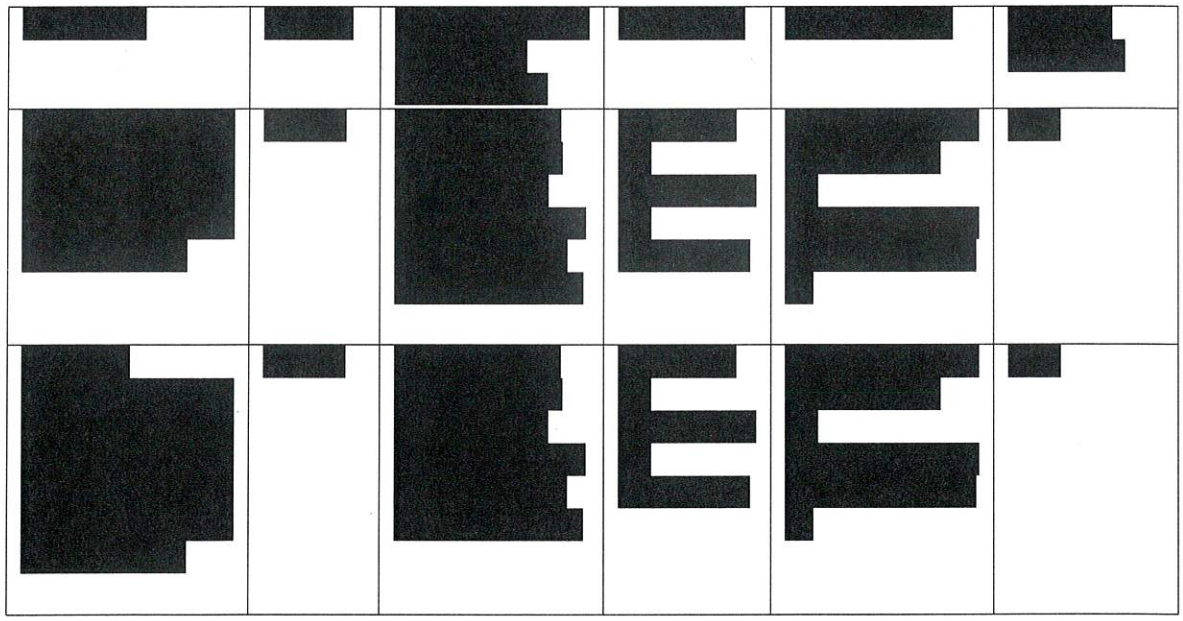


IV. Análisis de brecha

[redacted]

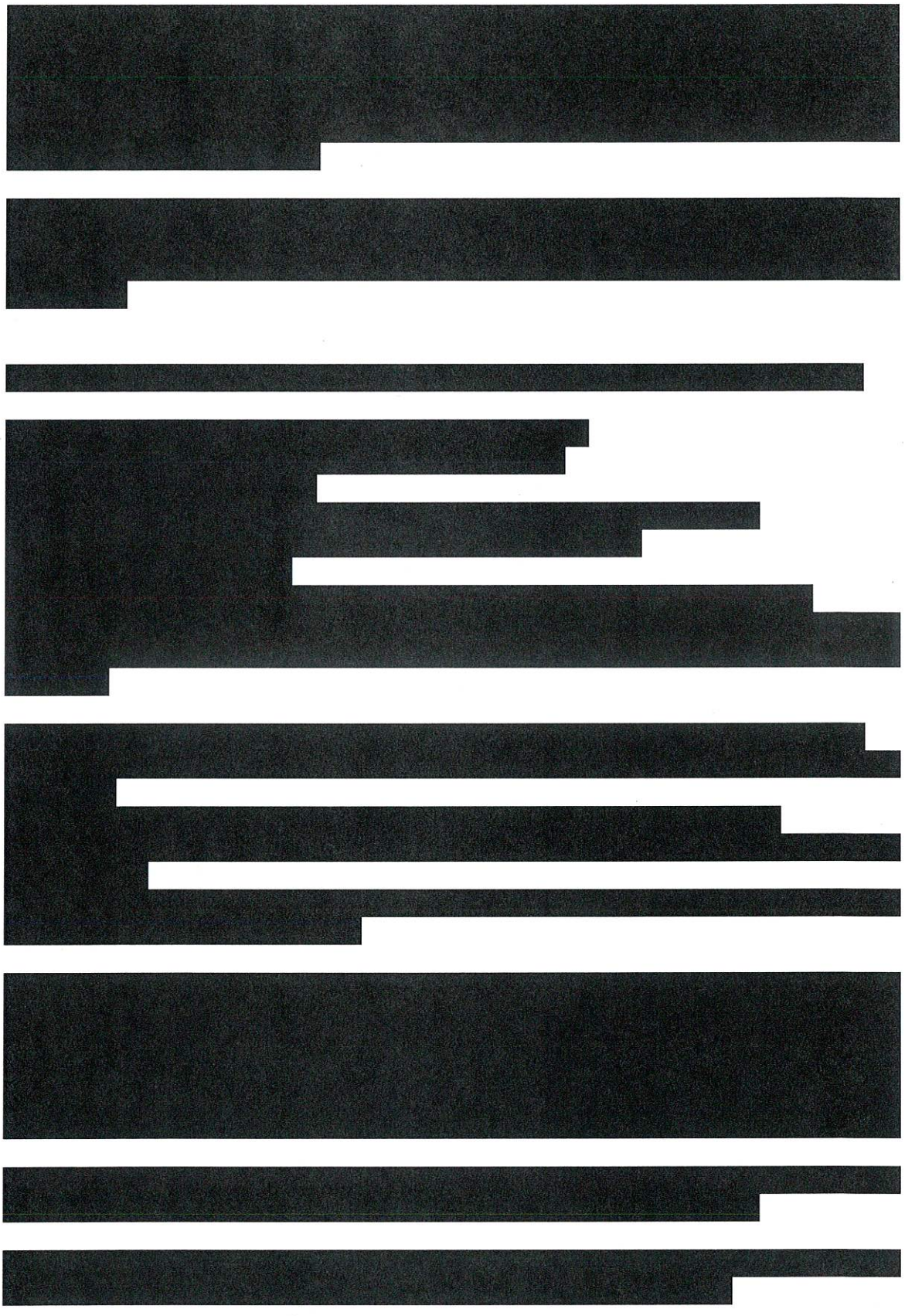
[redacted]

[redacted]



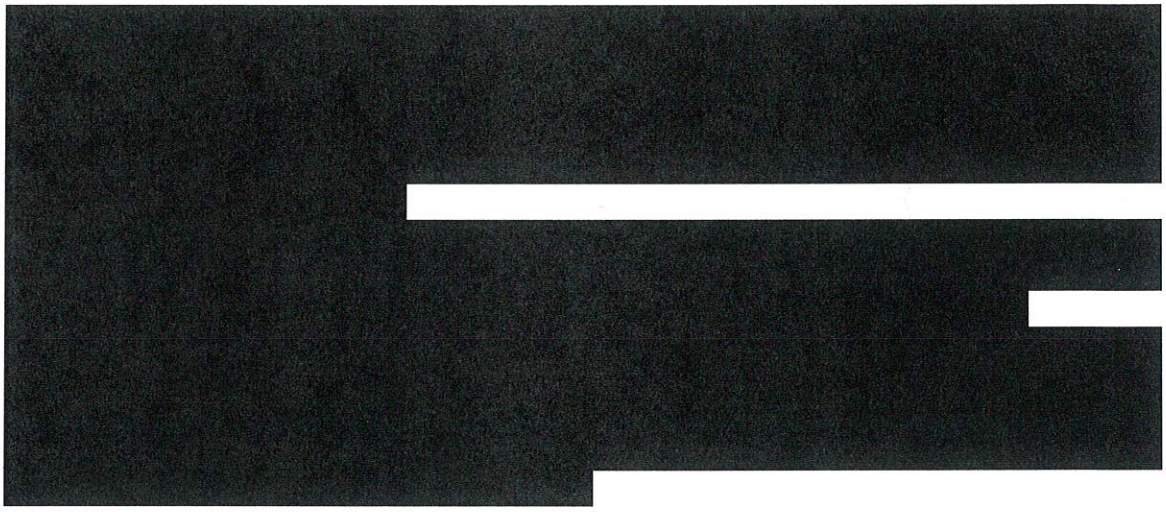
V. Plan de trabajo

[redacted]



VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad

[redacted]



VII. El programa general de capacitación.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales