INDICE

I.-INTRODUCCIÓN.

La Promotora para la Conservación y Desarrollo sustentable del Estado de Campeche, en su calidad de responsable, a fin de dar cumplimiento al deber de Seguridad y en completo apego a las disposiciones contenidas en el Capítulo III De los deberes y las medidas de seguridad de la Ley de Protección de Datos Personales en Posesión de los sujetos obligados del Estado de Campeche, ha establecido un conjunto de procesos y sistemas diseñados para la protección de los datos personales a los cuales tenga acceso a su tratamiento de acuerdo a sus funciones y atribuciones de Ley.

En tal sentido, dentro de las acciones a emprender en toda institución para cumplir con dicho deber, se actualiza el documento de seguridad, instrumento que dará cuenta de todas las medidas, acciones, actividades, controles o mecanismos, implementados por el responsable con el objeto de garantizar que el tratamiento de los datos personales que realiza sea conforme a las disposiciones contenidas en la normatividad de la materia.

Por lo anterior, la Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche (PROCDSCAM), procede a integrar y someter ante el Comité de Transparencia para su aprobación el presente Documento de Seguridad en cumplimiento a lo dispuesto por los artículos 55, 56, 124, párrafo segundo, y 125, fracción I, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche.

II.- GLOSARIO

ÁRCO: Acceso, Rectificación, Cancelación y Oposición.

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

Documento de seguridad: 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;

LPDPPSOEC: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

LTAIPEC: Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

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. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

PROCDSCAM: Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche.

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales

Titular: La persona física a quien corresponden los datos personales;

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

III.- NOMBRE DE LOS SISTEMAS DE TRATAMIENTO O BASE DE DATOS PERSONALES Y EL NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR.

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO O BASE DE DATOS PERSONALES	NOMBRE, CARGO Y ADSCRIPCIÓN DEL ADMINISTRADOR.
1.- Sistema de Recursos Humanos	C.P. Anaythe del Carmen Ojeda Balan.- Analista.-Encargada de Recursos Humanos.
2.- Sistema de contratos	C.P. David Garay Aguilar.-Nivel 5.1.Titular de Asuntos Jurídicos.
3.- Sistema de Actas	C.P. Hypatia Ek Moo.-Nivel 7.2. Titular de la Unidad de Transparencia.
4.- Sistema de Parque Recreativo Ximbal	Lic. Luis Manuel Moreno Aguilar.- Nivel .- Coordinador Administrativo.
5.- Base Sistema de Datos de Solicitudes de Información y solicitudes de Derechos ARCO	C.P. Hypatia Ek Moo.-Nivel 7.2. Titular de la Unidad de Transparencia.

IV.- FUNCIONES Y OBLIGACIONES DEL RESPONSABLE, ENCARGADOS Y TODAS LAS PERSONAS QUE TRATEN DATOS PERSONALES.

SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	FUNCIONES Y OBLIGACIONES
1.- Sistema de recursos humanos	Integración de expedientes personales de cada uno de los empleados que laboran en la PROCDSCAM, así como la administración de nómina, pago de impuestos, prestaciones y cuotas, revisión de auditorías, cumplimiento de obligaciones laborales ante otras autoridades (IMSS, INFONAVIT, etc.) y movimientos de personal.
2.- Sistema de contratos	Integración de expedientes de los proveedores con los que se ha contratado servicios (vigilancia, jardinería, limpieza, etc.) Integración de expediente de los Locatarios de Parque Campeche, con los que se ha celebrado contratos.
3.- Sistema de Actas	Integración de los expedientes de las Actas de la Junta de Gobierno de la PROCDSCAM
4.- Sistema de Parque Recreativo Ximbal	Integración de las fotos y actividades de la PROCDSCAM.
5.- Base Sistema de Datos de Solicitudes de Información y solicitudes de Derechos ARCO	Integración de los expedientes de las Solicitudes para ejercer sus Derechos de Acceso, Rectificación, Cancelación y Oposición de los datos personales.

V.-INVENTARIO DE DATOS PERSONALES TRATADOS EN CADA SISTEMA DE TRATAMIENTO Y/O BASE DE DATOS PERSONALES.

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	CATEGORIA DE DATOS PERSONALES	DATOS PERSONALES	FUNDAMENTO LEGAL
Pueden ser uno o más de acuerdo con los sistemas de datos que contempla el área	De conformidad con el numeral TERCERO de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, los cuales pueden ser datos: • De identidad • Electrónicos • Laborales • Patrimoniales • Sobre procedimientos administrativos o jurisdiccionales. • Académicos • De Tránsito y movimientos migratorios. • Sobre salud • Datos biométricos • Afectivos y/o familiares y datos personales de naturaleza pública.		Artículo 33 fracción IX de la LTAIPEC (Principio de Proporcionalidad)
Sistema de recursos Humanos	Datos de identidad	Nombre completo Domicilio particular Firma Registro Federal de Contribuyentes (RFC) Credencial INE	Artículo 33 fracción IX de la LTAIPEC (Principio de Proporcionalidad)
	Datos biométricos	Huella digital(reloj checador)	
	Datos electrónicos	Correo electrónico personal	
	Datos laborales	Nombramientos Incidencias Capacitaciones	
	Académicos	Curriculum	

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	CATEGORIA DE DATOS PERSONALES	DATOS PERSONALES	FUNDAMENTO LEGAL
Sistema de contratos proveedores	Datos de identidad	Nombre completo Domicilio particular Firma Registro Federal de Contribuyentes (RFC) Credencial INE	Artículo 33 fracción IX de la LTAIPEC (Principio de Proporcionalidad)
	Datos electrónicos	Correo electrónico personal	
	Datos patrimoniales	Información fiscal	
Sistema de convenios con Locatarios y módulos en Parque Campeche	Datos de identidad	Nombre completo Domicilio particular Firma Registro Federal de Contribuyentes (RFC) Credencial INE	Artículo 33 fracción IX de la LTAIPEC (Principio de Proporcionalidad)
	Datos electrónicos	Correo electrónico personal	
Sistema de Actas	Datos de identidad	Nombre completo Firma	
Base Sistema de Datos de Solicitudes de Información y solicitudes de Derechos ARCO	Datos de identidad	Fotografía	

VI.-ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO Y Y/O BASE DE DATOS PERSONALES SEÑALANDO EL TIPO DE SOPORTE Y LAS CARACTERÍSTICAS DEL LUGAR DONDE SE RESGUARDAN.

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	TIPO DE SOPORTE	CARACTERISTICAS DEL LUGAR DE RESGUARDO	PROGRAMAS EN LOS QUE SE UTILIZAN LOS DATOS PERSONALES
Sistema de Recursos Humanos	físico	Av. Lázaro Cárdenas S/N entre Av. Luis Donaldo Colosio y Calle Perú. Colonia Flor de Limón. C.P. 24069. Área Recursos Humanos	
	Electrónico:	Computadora de escritorio marca Dell	Paquetería office: Word, Excel y power point

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	TIPO DE SOPORTE	CARACTERISTICAS DEL LUGAR DE RESGUARDO	PROGRAMAS EN LOS QUE SE UTILIZAN LOS DATOS PERSONALES
Sistema de contratos proveedores	Físico	Av. Lázaro Cárdenas S/N entre Av. Luis Donaldo Colosio y Calle Perú. Colonia Flor de Limón. C.P. 24069. Área: Unidad Asuntos Jurídicos.	
	Electrónico:	Lap top marca	Paquetería office: Word, Excel y power point
Sistema de convenios con Locatarios y módulos en Parque Campeche	Físico	Av. Lázaro Cárdenas S/N entre Av. Luis Donaldo Colosio y Calle Perú. Colonia Flor de Limón. C.P. 24069. Área: Unidad Asuntos Jurídicos.	
	Electrónico:	Lap top	Paquetería office: Word, Excel y power point
Sistema de Actas	Físico	Av. Lázaro Cárdenas S/N entre Av. Luis Donaldo Colosio y Calle Perú. Colonia Flor de Limón. C.P. 24069. Área: Unidad de Transparencia	
	Electrónico:	Lap top, marca Dell	Paquetería office: Word, Excel y power point
Base Sistema de Datos de Solicitudes de Información y solicitudes de Derechos ARCO	Físico	Av. Lázaro Cárdenas S/N entre Av. Luis Donaldo Colosio y Calle Perú. Colonia Flor de Limón. C.P. 24069. Área: Unidad de Transparencia	
	Electrónico:	Lap top, marca Dell	Paquetería office: Word, Excel y power point

VII.- CONTROLES Y MECANISMOS DE SEGURIDAD PARA LA TRANSFERENCIAS.

En esta sección se describe la forma en la que se lleva a cabo la transferencia de los datos personales, que en su caso, se efectúen, señalando que personal es el autorizado para realizarla y recibirla, hacía que otra unidad administrativa los puede transmitir y que mecanismos se utilizan para llevar el control de dicha transferencia.

NOMBRE DE LOS SISTEMAS DE TRATAMIENTO Y/0 BASE DE DATOS PERSONALES	CONTROLES Y MECANISMOS DE SEGURIDAD
Transmisiones mediante el traslado de soportes físicos en el caso de la nómina del Sistema de Recursos Humanos	Cuando se transfiere información confidencial esta se realiza en sobre sellado, es realizado por la persona encargada del Área de Recursos Humanos.
Sistema de contratos proveedores	No se realiza la trasferencia de información de estos sistemas. La información es resguardada de manera física en los expedientes correspondientes y de manera digital en las computadoras.,
Sistema de convenios con Locatarios y módulos en Parque Campeche	
Sistema de Actas	
Base Sistema de Datos de Solicitudes de Información y solicitudes de Derechos ARCO	

(Formato No. 2 de los anexos).

VIII.- RESGUARDO DE LOS SOPORTES FÍSICOS Y/O ELECTRÓNICOS DE LOS DATOS PERSONALES.

Tipos de soportes: físicos y electrónicos

Es importante explicar la diferencia entre un soporte físico y uno electrónico debido a que las medidas de seguridad que los sujetos obligados implemente para cada sistema de datos personales están estrechamente relacionados con el tipo de soportes utilizados.

- **Soporte físico:** Son los medios de almacenamientos identificados a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos, fotografías, carpetas, expedientes, entre otras.

- **Soporte electrónico:** son los medios de almacenamiento que pueden ser comprendidos solo mediante el uso de algún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, video y datos, discos ópticos (CDs y DVDs), discos magnéticos y demás medios de almacenamiento masivo.

En esta sección se describe la forma en la que se realiza la transferencia de los datos personales, señalando que personal es el autorizado para realizarla y recibirla, hacía que otra unidad administrativa los transmite y que mecanismo se utilizan para llevar el control de.

a) Resguardo físico

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
ÁREA DE RECURSOS HUMANOS					
ARCHIVERO DE 3 CAJONES	ANAYTHE DEL CARMEN OJEDA BALAN	ANALISTA	SIN MARCA	METALICOS	S/N
UNIDAD DE ASUNTOS JURÍDICOS					
ARCHIVERO DE 4 CAJONES	DAVID GARAY AGUILAR	SUBDIRECTOR	SIN MARCA	METALICO COLOR BEIGE	S/N
ANAQUEL 3 NIVELES	DAVID GARAY AGUILAR	SUBDIRECTOR	SIN MARCA	S/M	S/N
UNIDAD DE TRANSPARENCIA					
REPISA	HYPATIA EK MOO	JEFE DE DEPARTAMENTO	SIN MARCA	S/M	S/N

b) Resguardo electrónico

EQUIPO	BAJO RESGUARDO	CARGO	MARCA	MODELO	SERIE
ÁREA DE RECURSOS HUMANOS					
COMPUTADORA DE ESCRITORIO	ANAYTHE DEL CARMEN OJEDA BALAN	ANALISTA			
UNIDAD DE ASUNTOS JURÍDICOS					
PROCESADOR DE COMPUTADORA	DAVID GARAY AGUILAR	SUBDIRECTOR			
UNIDAD DE TRANSPARENCIA					
PROCESADOR DE COMPUTADORA	HYPATIA EK MOO	JEFE DE DEPTO.	DELL		

IX.- BITÁCORAS DE ACCESO, OPERACIÓN COTIDIANA Y VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES.

Se utilizan bitácoras de acceso en soportes físicos únicamente en los casos en que el personal responsable de los sistema de tratamiento o base de datos personales requieran acceder a la información contenida en ellos, o bien, en los casos en los cuales tratándose de soportes físicos estos se encuentren en el archivo de concentración por haber fenecido si periodo de trámite, para lo cual se requerirá, además de la autorización del responsable del sistema de tratamiento o base de datos personales, la autorización del responsable del archivo de concentración, conforme a los procedimientos archivísticos establecidos.

Para los casos en que se requiera extraer **algún equipo de cómputo o cualquier otro activo electrónico** que contenga datos personales se deberá solicitar la autorización correspondiente mediante el llenado del Ejemplo de Formato No. 1 contenidos en los anexos.

Las bitácoras de acceso a los datos personales en soportes físicos deberán contener lo siguiente:

- Nombre y cargo a quien accede
- Área de adscripción
- Identificación del Expediente
- Fojas de Expediente
- Propósito del Acceso
- Fecha de Acceso
- Hora de Acceso
- Fecha de Devolución
- Hora de Devolución

(Formato No. 3 de los anexos).

Las bitácoras de vulneraciones a la seguridad deberán contener lo siguiente:

- Fecha del incidente;
- Nombre y cargo;
- Área de adscripción;
- Responsable del área;
- Sistema de tratamiento o base de datos personales vulnerada.
- Cantidad de titulares vulnerados;
- Soporte de la información vulnerada;
- Tipo de vulneración;
- Tipo de dato personal afectado;
- Nombre y firma de quien reporta;
- Nombre y firma del administrador del sistema.

(Formato No. 4 de los anexos).

X.- ANÁLISIS DE RIESGOS

De conformidad con los artículos 52, fracción IV, y 56, fracción IX, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche, resulta necesario realizar el análisis de riesgo de los datos personales y de los recursos involucrados de su tratamiento, con la finalidad e identificar el nivel de riesgo que se tiene en la PROCDSCAM , en relación con el tratamiento de datos personales, y poder implementar en consecuencias las medidas de seguridad que resulten necesarias .

La determinación del nivel de seguridad está asociada en forma directa con la sensibilidad del dato personal. Mientras más sensible sean los datos tratados, mayor rigor se debe aplicar en la protección de los mismos. Es pertinente indicar que las medidas de seguridad asociadas a los niveles son acumulativas. Por ejemplo, en el nivel medio se incluyen, además de las medidas de seguridad que corresponden a este nivel, las adoptadas en el nivel básico. En consecuencia, en el nivel alto se contendrán las correspondientes al nivel básico y al nivel medio, en adicción a las propias del mismo.

El nivel alto, corresponde a las medidas de seguridad aplicables a los sistemas de datos personales relacionados a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delito.

1) **Nivel de protección básico:** datos de identificación y Datos laborales.

2) **Nivel de protección medio:** datos patrimoniales; datos sobre procedimientos administrativos seguidos en forma de juicio o jurisdiccional; datos académicos; datos de tránsito y movimientos migratorios.

3) **Nivel de protección alto:** datos ideológicos, datos de salud, características personales, características físicas, vida sexual, origen étnico y racial.

Para tal efecto, se tomará como base de dicho análisis la Metodología de análisis de Riesgo BAA, propuesta por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). En sentido, toda vez que en el presente documento de seguridad se han identificado previamente los diversos de tratamiento y/o bases de datos existentes en la Institución, y los datos personales que en ellos se tratan, se procede a determinar, conforme a la metodología citada, lo siguiente:

PRIMERO. - el nivel de **riesgo por tipo de dato** (factor Beneficio) resultado de:

1) El Nivel de riesgo inherente por tipo de dato (conforme lo establece la metodología).

2) El volumen de titulares (cantidad de personas físicas sobre las cuales se tiene dicho dato).

TIPO DE DATOS PERSONAL (De acuerdo con los datos personales que el Sujeto Obligado trata en sus sistemas)	NIVEL DE RIESGO INHERENTE (Bajo, Medio, Alto)	VOLUMEN DE TITULARES (Se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales, es variable dependiendo del Sujeto Obligado)
Capacitaciones	Bajo	20
INE	Bajo	20
Certificado	Bajo	20
Correo electrónico personal	Bajo	20
Correo electrónico laboral	Bajo	20

Toda vez que mediante la tabla anterior ha quedado establecido el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se procede a identificar el nivel de riesgo por tipo de dato tratado en la PROCDSCAM, otorgándole a cada nivel de riesgo un valor numérico de 1 al 5, donde 1 es el nivel más bajo y 5 el más alto, lo cual se ejemplifica de la siguiente tabla.

RIESGO INHERENTE						
Reforzado	R	4	4	5	5	5
Alto	A	1	2	3	3	3
Medio	B	1	1	2	3	3
bajo	A	1	1	1	1	1
		<500	<5k	<50k	<500k	>500k
		VOLUMEN DE TITULARES				

A continuación, se detallan los niveles mencionados:

Riesgo por tipo de dato **Nivel 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.

No se transcriben cuando ocurren los niveles **2, 3, 4 y 5** toda vez que resulta innecesario al no actualizarse ninguna de tales circunstancias

De los datos proporcionados con anterioridad, se puede inferir lógicamente que el nivel de riesgo por tipo de dato (factor Beneficio) para la PROCDSCAM es igual a Riesgo de Tipo Dato bajo conforme a la Metodología de análisis de Riesgo BAA.

SEGUNDO. - El nivel de riesgo por la cantidad de accesos potenciales a los daros personales (factor Accesibilidad).

Establecido el nivel de riesgo por tipo de dato, procede determinar el nivel de riesgo por tipo de acceso, determinado por la cantidad de accesos potenciales a los datos personales que se pretenden proteger, es decir, definiendo cuántas personales tienen la posibilidad de acceder a la información en un intervalo de tiempo determinado, conforme a la siguiente tabla:

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

De lo anterior, y toda vez se conoce que la cantidad de personas que laboran actualmente en cada una de las áreas involucradas en el tratamiento de datos personales es menor a veinte, resulta evidente que para la PROCDSCAM el nivel de riesgo por cantidad de accesos potenciales es BAJO.

TERCERO. - El nivel de riesgo por tipo de entorno (factor Anonimidad).

El factor anonimidad 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, determinándose en tal sentido el nivel de riesgo por el tipo de entorno, en el que, teniendo una escala del 1 al 5 , en donde 1 implica baja anonimidad y 5 mayor anonimidad del atacante, entre mas 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

XI.- ANALISIS DE BRECHA

El análisis de brecha es una herramienta de análisis para comparar el estado y desempeño real de una organización, estado o situación en un momento dado, respecto a uno o más puntos de referencia seleccionados; por lo que en esta sección se describirán las situaciones de las áreas de oportunidad para evitar posibles vulneraciones.

- En la gestión de usuarios y contraseñas de los equipos informáticos: Los riesgos de no contar con usuario y contraseña de los equipos en donde se resguarden Datos Personales se corre el riego de que la información sea vulnerada.
- En uso de medios de almacenamientos extraíbles: Los riesgos al permitir el acceso de almacenamientos extraíbles es que se puede hacer una copia digital de la información de los Datos Personales que se tiene resguardados.
- En el acceso a las instalaciones de la institución. Los riesgos al permitir el acceso de personal ajeno al área que resguarda la información de los Datos Personales, es el robo, daño o extravío de información.
- En el archivo de concentración. *La información en el archivo de concentración debe ser solo con la autorización del Encargado del Archivo de concentración, previo registro en la Bitácora de préstamos.*

XII. GESTION DE VULNERACIONES

Plan de respuesta

- Restauración inmediata de la operatividad mediando los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos.
- En caso de que la vulnerabilidad fuera resultado de la comisión de un delito realizar las denuncias correspondientes.
- Llenado de formato No. 4 (anexo), por parte de la persona que detecto la vulneración.

- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.

- Elaboración de informe y propuesta de medidas correctivas o cortos y mediano pazo por parte de la Unidad de Transparencia.
- Notificación a titulares en un lapso de 72 horas que de forma significativa vea afectados sus derechos patrimoniales o morales.
- Llenado de la bitácora de vulneraciones conforme al artículo 59 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

XIII. MEDIDAS DE SEGURIDAD IMPLEMENTADAS.

En término del artículo 3 fracción xxv DE LA Ley de protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Campeche, la medidas de seguridad son un conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales, sujetos a tratamientos al interior del responsable, y de los que se transfieran o remitan por diversas vías, a saber, las medidas de seguridad que actualmente se aplican son las siguientes:

a. Medidas de seguridad físicas

Para garantizar la seguridad física de las instalaciones, personas y equipos de la institución se cuenta con cuenta procedimientos de control y prevención ante amenaza s al entorno físico de los datos y de los recursos involucrados en su tratamiento, los cuales se describen a continuación:

	Medidas	Finalidad	Descripción
Medidas de seguridad físicas	Seguridad privada en edificio sede	• Prevenir el acceso no autorizado al perímetro de las oficinas de la PROCDSCAM. • Prevenir el daño o interferencia a las instalaciones. • Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	Las instalaciones son resguardadas por elementos de vigilancia privada, miembro de la persona moral con la que se tiene firmado contrato de prestación de tal servicio, en horas hábiles inicia a las 07:00 horas de cada día y termina a las 07:00 horas del día siguiente, u en días inhábiles las 24 horas al día.
	Instalación de cámaras de	• Prevenir el acceso no autorizado al	Las instalaciones cuentan con sistema de video-vigilancia que consta de 7 cámaras

	videos vigilancia	perímetro de la organización. • Prevenir el daño o interferencia a las instalaciones. • Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	ubicadas en sitios estratégicos o acceso a las instalaciones.
	Barda perimetral	• Prevenir el acceso no autorizado al perímetro de la organización. • Prevenir el daño o interferencia a las instalaciones. • Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	Las instalaciones cuentan con un barda perimetral de aproximadamente de 3 metros de altura que cubre la totalidad de las instalaciones, y cuentan con 4 accesos (entrada principal, filtro, domos y bodega)
	Acceso a unidades administrativas	• Prevenir el acceso no autorizado al perímetro de la organización. • Prevenir el daño o interferencia a las instalaciones. • Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	Las unidades administrativas cuentan con puertas de acceso con cerraduras, las llaves se encuentran bajo resguardo del titular del área administrativa. Fuera del horario oficial de labores, salvo situaciones extraordinarias, las puertas de acceso a las unidades administrativas se deben mantener cerradas bajo llave.
	Seguridad física de equipos	• Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico	Los equipos de cómputo se sitúan sobre superficies fijas, mesas de trabajo y escritorios, a una altura adecuada para evitar caídas daños por estas. Los equipos de cómputo se ubican lejos de ventanas para evitar que objetos lanzados desde el exterior caigan sobre ellos y los dañen. Tanto los equipos de cómputo (soportes electrónicos) como archiveros (soportes físicos) cuentan el debido cuidado por parte del servidor público del cual se encuentran bajo resguardo. En las plantas altas y bajas de las instalaciones se cuentan con extintores de incendios, conforme al plan interno de

			protección civil.

b. Medidas de seguridad técnicas

Para garantizar la seguridad técnica y operativa de los recursos tecnológicos (hardware y software) involucrados en el tratamiento de datos personales se realizan e implementan las acciones y mecanismos siguientes:

	Medidas	Finalidad	Descripción
Medidas de seguridad técnicas	Usuarios y contraseñas	Prevenir el acceso a los datos personales, así como a los recursos, sea por usuarios identificados y autorizados; generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.	Los equipos de cómputo asignados a cada servidor público para el desempeño de sus funciones, cuentan con contraseña de encendido y contraseña de usuario.
	Software de seguridad	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.	Todos los equipos de cómputo cuentan con programas antivirus bajo licencia. Los registros de renovación de licencia o cambio de software corren a cargo de la coordinación administrativa.
	Mantenimiento de equipos.	Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.	Realizar de manera periódica el mantenimiento preventivo o, en su caso, correctivo de los equipos de cómputo en los cuales se tratan datos personales.

c. Medidas de seguridad Administrativas

Para garantizar la seguridad administrativa de los datos personas en la gestión de los procesos a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales, así como la

sensibilización y capacitación del personal en materia de protección de datos personales se toman las siguientes medidas:

	Medidas	Finalidad	Descripción
Medidas de seguridad Administrativas	Capacitación general y particular	Sensibilizar y capacitar al personal en materia de protección de datos personales. Que el personal conozca y cumpla con los principios, deberes, derechos y demás obligaciones en la materia y las sanciones en caso de incumplimiento.	*Todos los empleados deben recibir una capacitación sobre aspectos generales de la ley en materia al manejo una vez por año y los nuevos colaboradores en sus primeros días de entrar en funciones.*
	Establecer políticas y procedimientos para la gestión, soporte y revisión de la seguridad de los datos personales a nivel organizacional, la identificación, clasificación y borrado seguro de los datos personales.	Delimitar las actuaciones en la gestión de los procedimientos internos. Establecer los principios que rigen el actuar de los servidores públicos de la PROCDSCAM.	*Enunciar las disposiciones normativas, tales como Código de Ética, Código de conducta de los servidores públicos, reglamento interior, manual de organización, manual de procedimientos, etc.*

XIV.- CONTROLES DE IDENTIFICACION Y AUTENTIFICACION DE USUARIOS

Los servidores públicos trabajadores de la PROCDSCAM en todo momento deberán portar el uniforme y contar a su vez con gafetes identificativos, los cuales deberán contener:

Al frente:	Al reverso:
 • Nombre	• Vigencia • Número de empleado • Firma del (de la) Director (a) General

• Cargo • Fotografía • Área de adscripción	• Datos dela PROCDSCAM • Domicilio Institucional • Teléfono institucional

XV.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACION DE DATOS PERSONALES

El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, ello para en caso de que primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar perdida generalizada de datos.

Los respaldos que se realicen de manera periódica deberán registrarse en la bitácora de respaldos, que estará a cargo de los servidores públicos que tengan asignados equipos de cómputo.

(Formato No. 5 de los anexos).

XVI.- PLAN DE CONTINGENCIA

Es un conjunto de estrategias diseñadas para ser aplicadas, durante y luego de la presentación de una emergencia a fin de minimizar los daños que pueden ocasionarse tanto al personal a cargo como a la información.

Estas medidas están incluidas en el Programa Interno de Protección Civil de la PROCDSCAM que estará sujeto para aprobación de la Secretaria de Protección Civil (SEPROCI), el cual implica un análisis de los posibles riesgos a los cuales puede estar expuestas nuestra información contenida en los diversos medios de almacenamiento de los sistemas de tratamiento o base de datos personales dependiendo del grado de emergencia.

a) Unidad Interna de Protección Civil.

Se conformará la Unidad de Protección Civil esta instancia será el primer contacto con los cuerpos de emergencias en las tareas de protección civil de la PROCDSCAM y la máxima autoridad en la materia al momento de presentase un alto riesgo, emergencia, siniestro o desastre, el cual tendrá as siguientes funciones:

- Coordinar las acciones de protección civil en la comisión ante situaciones, riesgos y emergencias.
- Elaborar y coordinar el Programa Interno de Protección Civil.
- Difusión del documento una vez aprobado.
- Integrar la Unidad Interna de Protección Civil de la PROCDSCAM.

- Se debe contar con un responsable general quien guiará la implementación del mismo, así como la toma de las decisiones.
- Seleccionar a los integrantes de las brigadas que conformarán la Unidad Interna de Protección Civil.
- Elaborar programas de actividades de capacitación y difusión.
- Identificar, analizar y evaluar riesgos internos y externos
- Supervisar, elaborar y actualizar directorio de emergencias.
- Concertar acuerdos con autoridades fuera de las instalaciones
- Promover la capacitación coordinando charla sobre prevención, atención y recuperación de desastres a todo el personal involucrado en el Programa Interno de Protección Civil.

b) Medidas de prevención y conservación de archivos.

- Espacios con luz natural y sin humedad
- Los muebles de archivo deben garantizar la conservación de los documentos que guardan, los documentos deben guardar uniformidad.
- Evitar archivar documentación cerca de aparatos eléctricos, las instalaciones eléctricas deben estar en buenas condiciones.
- Los estantes de los archivos deben estar entre 10 y 15 cm del suelo (facilitan la limpieza y evita su vez acumulación de humedad y proliferación de plagas).
- Todos los equipos eléctricos deben quedar apagados y desconectados durante la noche o cuando no se utilicen.
- Se recomienda no colocar vasos con líquido que puedan derramarse fácilmente sobre los aparatos eléctricos.
- Contar con un extintor cerca del Archivo de Concentración.
- Contar con detector de humo en las unidades administrativas en especial en el Archivo de Concentración.

c) Medidas preventivas ante siniestros.

- INCENDIO: Si detecta un incendio procura la calma y repórtelo inmediatamente a la brigada de prevención y combate de incendios para que atiendan la emergencia conforme a la planificación.

Durante un incendio:

- Si el incendio es pequeño, se procurará apagarlo mediante un extintor.
- Si el fuego es de origen eléctrico no se deberá intentar apagarlo con agua.
- No abra puertas ni ventanas el fuego se extiende con el aire.
- Si el incendio no se puede controlar solicitar apoyo a lo bomberos.
- No pierda tiempo buscando objetos personales y salga del inmueble lo ante posible.
- Si hay gas o humo humedezca un trapo cubriendo nariz y boca.
- Si su ropa se enciende; tírese al piso y ruede lentamente.

Después del incendio:

- Mantener suspendida la corriente eléctrica, el agua y el gas hasta que se revise el estado del inmueble sus instalaciones y los servicios en general.
- Para regresar al anterior del inmueble, es necesario que las personas responsables de protección civil otorguen la autorización y sea seguro.

Resguardo de la información en caso de incendio:

- Respaldo de información en una zona de preferencia, donde el calor de un incendio no alcance los dispositivos, esto es en lugares cercanos a los extintores (sugerencias para realizar el almacenamiento de la información: CD, Disco duro, dispositivos de almacenamiento, la nube únicamente si es segura).
- Tener identificados los documentos con mayor valor para resguardarlos en una zona segura (realizar la digitalización de los mismo con resguardo en la nube si es segura o en dispositivos de almacenamientos)

  .
- **INUNDACIONES:** Para evitar pérdidas graves es importante realizar la revisión y reparación de ventanas y puertas, por donde podría filtrarse el agua de lluvia, así como impermeabilizar los techos en temporadas de lluvias estos para evitar goteras.

Previamente:

- Evitar colocar expedientes y/o documentos directamente sobre el piso.
- Respetar, al menos, una altura de 10 a 15 cm de los archiveros.
- Colocar barreras para el agua (cubrir los documentos de las goteras).
- Evacuar los documentos afectados hacia áreas ventiladas.

- Inmediatamente colocar papel secante en cada hoja de los expedientes.
- Si un documento en papel se moja en su totalidad se puede secar individualmente mediante ventilación o realizar la congelación del mismo para su recuperación, debe realizarlo preferentemente un especialista.

Durante una inundación:

- Desconectar servicios de luz, gas y agua.
- Mantenerse alejados de árboles y postes de luz.
- Evitar tocar o pisar cables eléctricos.
- Cubrir aparatos u objetos que puedan dañarse con el agua.

Después de la Inundación:

- Expulsar el agua mediante esponjas, baldes, recogedores, en el caso de no contar con una bomba con motor de combustión.
- Cerciorarse de que los aparatos eléctricos estén secos antes de utilizarlos nuevamente.
- Desinfectar las áreas afectada pisos, muros y mobiliario rescatable, con agua, jabón y cloro para evitar enfermedades.
- Ventilar las áreas afectadas después de la inundación.
- Identificar documentos dañados con la inundación y proceder a aplicar medidas para recuperarlo.
- Reportar lo que se dañó con el paso de la inundación.

- **AMENAZAS INFORMÁTICAS:** Ante un evento informático los pasos a seguir para mantener la seguridad de la información, son los siguientes:
    - Cambiar contraseña
    - Las contraseñas no deben contener información personal como nombre real, nombre de usuario, fechas de nacimiento o incluso el nombre institucional.
    - Deben ser muy distinta a tus contraseñas previas.

Para la atención ante una situación de emergencia de este tipo se utilizarán los siguientes elementos:

1. ***Brigada de prevención y combate de incendios:*** intervendrán con los medios disponibles para tratar de evitar que se produzcan daños y pérdidas en las instalaciones de la comisión como consecuencia de una amenaza de incendio.

2. ***Sistema de alarma:*** se ubicarán alarmas en lugares estratégicos, las cuales advertirán al personal a presencia de un peligro.

3. ***Detectores de Humo:*** Se ubicará en el Archivo de Concentración e Histórico, en su caso.

4. ***Equipos contra incendios:*** En las instalaciones se dispondrán y ubicarán extintores en un lugar visible y de fácil acceso.

5. Se deberá tener acceso al ***botiquín*** para realizar tratamientos de primeros auxilios.

6. La brigada de prevención y combate de incendios se encargará del manejo de los extintores, supervisará el mantenimiento de equipos contra incendio y será el personal capacitado para esta emergencia.

7. Mientras se está conectado a internet el atacante tendrá acceso a los archivos e información guardados en la computadora vulnerada, por lo que recomienda desconectar el cable de la red lo antes posible.

XVII.- TECNICAS DE SUPRESION Y BORRADO SEGURO DE LOS DATOS PERSONALES

Los métodos físicos	***Trituración:*** mediante una máquina trituradora se cortará cada uno de los documentos de forma vertical, lo cual hace prácticamente imposible que se pueden unir. ***Destrucción de los medios de almacenamiento electrónicos mediante desintegración:*** separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
Métodos lógicos	***Sobre-escritura:*** escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes.

XVIII.- PLAN DE TRABAJO

De las medidas de seguridad faltantes por implementar se realizará un análisis para determinar el tiempo promedio para ser subsanadas, dicho periodo no podrá ser mayor de 24 meses una vez aprobado el presente ***Documento de Seguridad***, tales adecuaciones se sujetaran, en el caso que requerir la erogación de recursos económicos, a las previsiones presupuestarias existentes, las medidas que no requieran la erogación de recursos

deberán ser implementadas a partir de la aprobación del presente ***Documento de Seguridad*** y la vigilancia de su debida observancia estarán a cargo del ***Comité de Transparencia*** y la ***Unidad de Transparencia***, para lo que todas las unidades administrativas de la Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche deberán presentarles las facilidades necesarias para implementación, vigilancia y evaluación de las medidas de seguridad implementadas y de las necesarias por implementar al interior de la PROCDSCAM.

XIX.- MECANISMOS DE MONITOREO Y REVISION DE LAS MEDIDAS DE SEGURIDAD

Informe anual	Se realizara un informe detallado de las medidas de seguridad existentes de manera anual por parte del ***Comité de Transparencia*** y la ***Unidad de Transparencia***, para valorar el estado que estas guardan, durante mes de enero de cada año.

XX.- PROGRAMA GENERAL DE CAPACITACION

El programa de capacitación actualiza a los servidores públicos de los responsables y de la propia PROCDSCAM, en materia de Protección de Datos Personales, de conformidad con lo establecido por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Campeche.

Estrategias de capacitacion	
Capacitacion permanente **Capacitacion focalizada**	Implementar entre los servidores publicos de Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche cursos sobre aspectos generales de la Ley de Proteccion de Datos de Posesion de Sujetos Obligados del Estado de Campeche.
Acciones de capacitacion a responsable de tratamiento	
Proporciona a los servidires publicos las herramientas necesaria que les permitan mejorar las gestion de la proteccion de datos personales a fin de incrementar los niveles de seguridad en el tratamiento de datos personales al interior de la institución.	
Impartido por: COTAIPEC, CEVINAI y/o Unidad de Transparencia del Sujeto Obligado. *Dirigido a:* Integrantes del Comité de Transparencia,	Aspectos Generales de la Ley de Proteccion de Datos Personales en Posesion de Sujetos Obligadoss. Lineamientos para la Proteccion de Datos Personales en Posesion de Sujetos Obligados del Estado de CAMPECHE.

Tiulares de las unidades administrativas, y cualqier otro personal involucrado en el tratamiento de datos personales al interior de la PROCDSCAM.	Derecho ARCO Documento de seguridad y Aviso de Privacidad. Proteccion de Datos Personales en Redes Sociales.

ANEXOS:

Formato No. 1	Vale de ingresos / salida de equuipos de cómputo
Formato No. 2	Bitacoras de transferencias.
Formato No. 3	Bitácorasde Acceso a datos personales en soportes físicos.
Formato No. 4	Vulneraciones a la seguridad de datos personales.
Formato No. 5	Procedimientos de respaldo y recuperación de datos personales.

FORMATO NO. 1

VALE DE INGRESOS / SALIDA DE EQUIPOS DE CÓMPUTO

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTBLE DEL ESTADO DE CAMPECHE				
		No. de Folio:		Fecha:
Nombre y cargo del solicitante				
Área de adscripción				
Descripción del equipo	Marca	Modelo	Serie	No. de inventario
Salida del equipo de cómputo				
Fecha: _____ Hora: _____				
El bien es propiedad de la Comisión: Si ☐ No ☐				
Nombre del responsable del equipo:				
Motivo del préstamo: Reparación ☐ Comisión ☐ Otro:_____				
Tiempo aproximado del préstamo: _____				
_____ Firma del solicitante			_____ Firma del responsable del equipo	
Devolución del equipo de computo				
Fecha: _____ Hora: _____				
Descripción del equipo				

Firma del solicitante

Firma del responsable del equipo

FORMATO No. 2

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTBLE DEL ESTADO DE CAMPECHE

BITÁCORA DE TRASFERENCIAS

Fecha	*Medio*	*Datos personales trasferidos*	*Receptor*	*Persona que recibe*	*Autorización*

FORMATO No. 3

BITACORA DE ACCESO A DATOS PERSONALES EN SOPORTES FÍSICOS

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTBLE DEL ESTADO DE CAMPECHE				
		No. de Folio:		Fecha:
Nombre y cargo de quien accede al expediente				
Área de adscripción				
IDENTIFICACIÓN DEL EXPEDIENTE				
NOMBRE DEL EXPEDIENTE	Sección	Serie	Subserie	Fojas del expediente
Datos del Acceso:				

Fecha: _____ Hora: _____

Motivo del Acceso:

Tiempo aproximado del préstamo: _____

_____ _____

Firma de autorización del Archivo de concentración

Firma del responsable del Sistema de Tratamiento o base de datos personales.

Devolución del expediente:

Fecha: _____ Hora: _____

_____ _____

Firma del responsable del Archivo de concentración	Nombre y firma de quien accede

NOTA: Únicamente será en caso que el expediente se encuentre en el Archivo de Concentración por haber fenecido su periodo de trámite, para lo cual se requiere previa autorización del responsable del sistema de tratamiento o base de datos personales y del responsable del Archivo de Concentración, conforme a los procedimientos archivísticos establecidos.

FORMATO No. 4

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTBLE DEL ESTADO DE CAMPECHE

VULNERACIONES A LA SEGURIDAD DE DATOS PERSONALES

Vulneraciones a la seguridad de datos personales	
FECHA DEL INCIDENTE	
NOMBRE Y CARGO	
Área de adscripción	
Responsable del área	
Sistema de tratamiento o base de datos personales vulnerada	
Cantidad de titulares vulnerada	
Soporte de la información vulnerada	Físico ☐ Electrónico ☐ Ambos ☐
Tipos de vulneración	☐ Perdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada
Tipo de dato personal afectado	☐ Identidad ☐ Académico ☐ Electrónico ☐ Laboral ☐ Patrimonial ☐ Salud

	☐ Procedimientos administrativos o jurisdiccionales ☐ Tránsito y movimiento migratorio ☐ Biométricos ☐ Naturaleza publica ☐ Afectivos y/o familiares
_____ Firma del solicitante	_____ Firma del responsable del equipo

FORMATO No. 5

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTBLE DEL ESTADO DE CAMPECHE

PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS PERSONALES

ÁREA:		EQUIPO:				
		SERIE:				
Nombre y cargo del responsable del equipo	Fecha	Hora	Tipo			Observaciones
			A	B	C	

A RESPALDO COMPLETO.- Respaldo de todos los ficheros y directorios
B RESPALDO DIFERENCIAL.- Respaldo de todos los ficheros y directorios modificados desde el último respaldo completo.
C RESPALDO INCREMENTAL.- Respaldo de todos los ficheros y directorios modificados desde el último respaldo.