	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRS115

CONTROL DE CAMBIOS

Cambio de Formato a partir del PGCRC02 Elaboración de información Documentada
 Antes POL-SIS-03 Política cifrado de datos
 Organización de la información
 Se agrega el Resguardo de llaves antes POL-SIS-04 Resguardo de llaves

1. OBJETIVO

Garantizar el uso adecuado y eficaz de las técnicas criptográficas para asegurar la confidencialidad, integridad y autenticidad de la información sensible manejada por Comercializadora Rápido S.A. de C.V., tanto almacenada como en tránsito.

2. ALCANCE

Cubre a todos los activos que almacenen información y a la aplicación de cifrado de datos de las operaciones y a cualquier persona que tenga acceso a los sistemas para el cifrado de datos de Comercializadora Rápido S.A. de C.V.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
 Cid Palacios Jesús David Administrador de infraestructura	 Pitol Pimentel Carlos Adrián Gerente de Sistemas	 Martínez Ponce Janely Gestión de Calidad	 Montes Barrera Elliioth Abdel Gerente General

3. REFERENCIAS

ISO 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

4. DEFINICIONES Y ABREVIATURAS

4.1 Sistema de Información:

Conjunto discreto de tecnología de la información organizado para la recopilación, procesamiento, mantenimiento, uso, divulgación, destrucción o eliminación de la información.

4.2 Llave:

En criptografía, es una parte de la data que te da la capacidad de cifrar o descifrar un mensaje.

4.3 Llave pública:

Utilizada por numerosos algoritmos criptográficos y criptosistemas, cuyos caracteres distintivos con la utilización de algoritmos de llaves asimétricas.

4.4 Certificado:


Es un archivo firmado con clave privada de una autoridad que contiene la clave pública de dicha identidad y los atributos del titular del certificado.

4.5 Cifrado de datos:

Es la conversión de datos de un formato legible a un formato codificado.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 1 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15

4.6 Cifrado simétrico/Llave privada:

Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano.

5. RESPONSABILIDADES

5.1 Gerente General

Aprobar la información documentada del SGC, asegurando que los recursos necesarios estén disponibles para lograr sin problema la implementación efectiva del documento.

5.2 Gerente Sistemas IT

Es responsabilidad de Gerencia de Sistemas IT gestionar las claves y certificados del cifrado que se utilicen en el almacenamiento y transmisión de la información.

5.3 Administrador de Base de datos.

Es responsabilidad de Administrador de la base de datos garantizar la seguridad, administración y monitoreo, de los datos cifrado y gestión de la misma. Responsable de generar y distribuir las llaves y certificados del cifrado, controlar los accesos e identificarlos.

5.4 Administrador de Infraestructura.

Es responsabilidad de Administrador de infraestructura gestionar la infraestructura de servidores asegurando la continuidad operativa del software instalado en los servidores tales como el software de Oracle, Base de Datos, de seguridad de la red, de antivirus, de comunicación con Internet, etc.

5.5 Gestión de Calidad

Gestionar el cumplimiento documental según lo establecido en el SGC, asegura su adecuada implementación, manteniendo la eficacia, así como la mejora continua de estas, resguardando y emitiendo la documentación controlada.

6. DESARROLLO

Se debe de cumplir lo establecido en las **Políticas de cifrados de datos PECSI15_PO01(3)**.


6.1 Información susceptible de ser cifrada

Dicha información puede ser:

- Información sensible, de carácter personal o confidencial.
- Registros con credenciales de autenticación.
- Información transferida a través de almacenamientos físicos no protegidos adecuadamente.
- Documento que contiene información personal y privada de un individuo, empresa, números de cuenta, datos personales, contraseñas, claves privadas de acceso a los sistemas y/o algún dato que pueda presentar una vulnerabilidad a la seguridad de la información.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 2 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRS115

6.1.1 Uso de firma electrónica

Se hará uso de la firma electrónica en aquellos escenarios en los que sea imprescindible garantizar la autenticidad, como para realizar trámites con las Administraciones Públicas o emisión de facturas.

6.1.2 Certificados web (Metodología)

Para garantizar la seguridad de la información en nuestros Web Service, adquiriremos un certificado web (SSL EV) para validación de dominio, de la organización y validación extendida y garantizar la seguridad.

Se siguen los siguientes pasos para realizar los certificados Web, siendo el responsable el Administrador de base de datos

ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD	REGISTRO
Agregar certificado al sitio Web/Servicio	Abrir el administrador de servicios windows, seleccionar el sitio al que se agrega certificado, se carga certificado en Formato Zip y se completa solicitud de certificado.	N/A
Verificar la instalación.	Se valida el acceso al sitio a través del prefijo HTTPS.	El certificado es otorgado por el proveedor externo AKKY . Y posteriormente se almacena en los servidores locales.

6.1.3 Cifrado de datos sensibles en desarrollos de aplicaciones

Para las aplicaciones que manejan información sensible, deberán contar con acceso (login), y las claves de acceso se almacenarán cifradas dentro de las bases de datos para mantener su integridad.

Para el uso de las llaves de encriptación se manejará un cifrado simétrico que contenga una longitud mínima de 12 caracteres y una longitud máxima de 30 caracteres.

Se siguen los siguientes pasos para cifrados de datos sensibles, siendo el responsable el Administrador de Base de datos.


ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD	REGISTRO
Recibe la información a almacenar de la transacción.	A través de un stored procedure se envía la información sensible a la base de datos.	Base de datos correspondiente a la encriptación.
Se realiza el encriptado de la información a través de un encriptado de 2 vías	Se utiliza una función propia del gestor de base de datos que proporciona funciones criptográficas para postgre SQL.	Base de datos correspondiente a la encriptación.

6.1.4 Acceso desde el exterior con VPN

En caso de la necesidad de trabajo fuera de las instalaciones se solicita el acceso a Gerencia General vía correo electrónico; de ser autorizada se configura el acceso de conexión VPN por parte del administrador de infraestructura.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 3 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

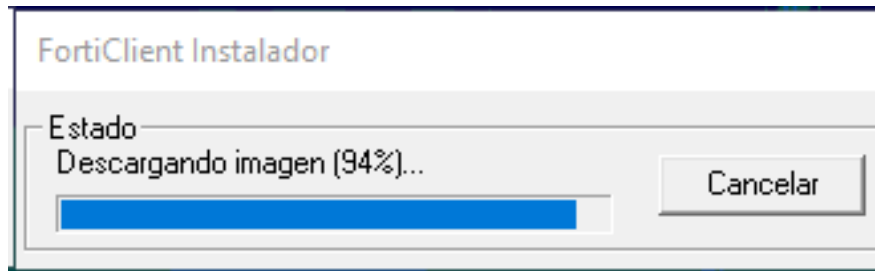
	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRS115

Si autorizamos el acceso desde el exterior a los servidores de nuestras instalaciones, tendremos que habilitar canales VPN de tipo IPSEC cifrados que garanticen la confidencialidad e integridad de las comunicaciones siguiendo la Política de uso de Wi-Fi y conexiones externas.

6.2 Metodología de cifrado

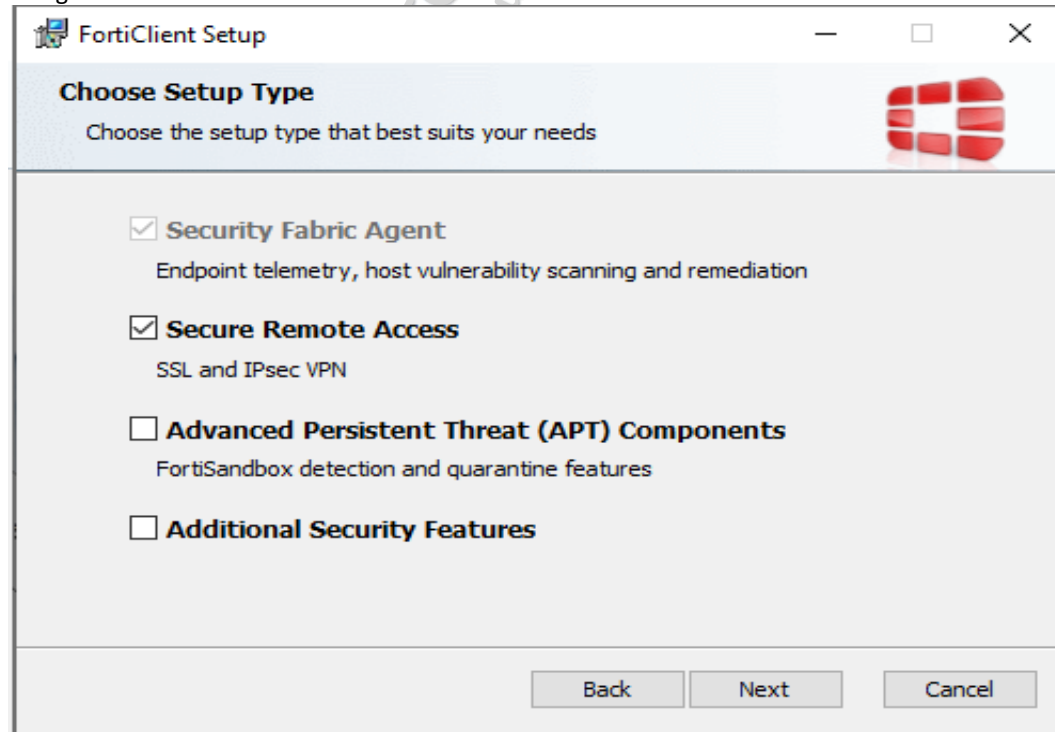
Se instala la aplicación FortiClient de proveedor externo Fortigate del equipo que requiere ser vinculado a la VPN.

Ejemplo: Instalación de FortiClient



Se ejecuta la aplicación de FortiClient en automático y se aceptan los términos y condiciones de la aplicación, se selecciona Acceso Remoto Seguro (Secure Remote Access).


Ejemplo: Configuración de FortiClient



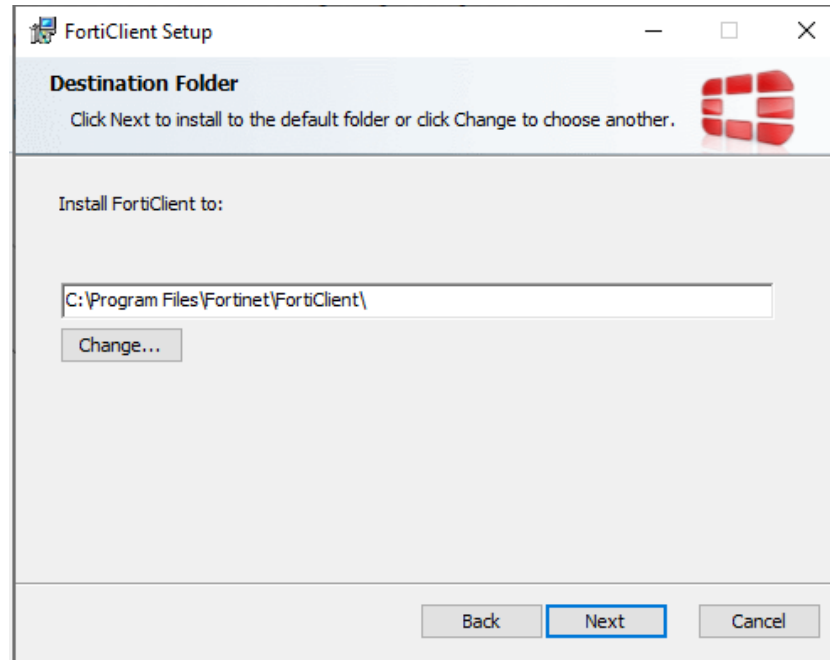
Selección de la ubicación que por default a la unidad C.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 4 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRS115

Ejemplo: Configuración de FortiClient




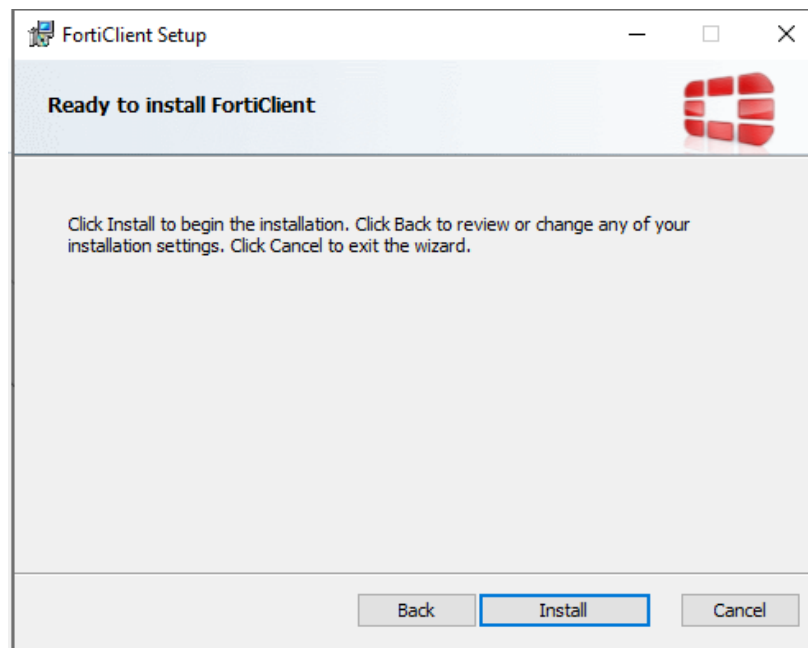
Instalar y finalizar.

Ejemplo: instalar

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 5 de 12
--	-----------------------	---------------------------

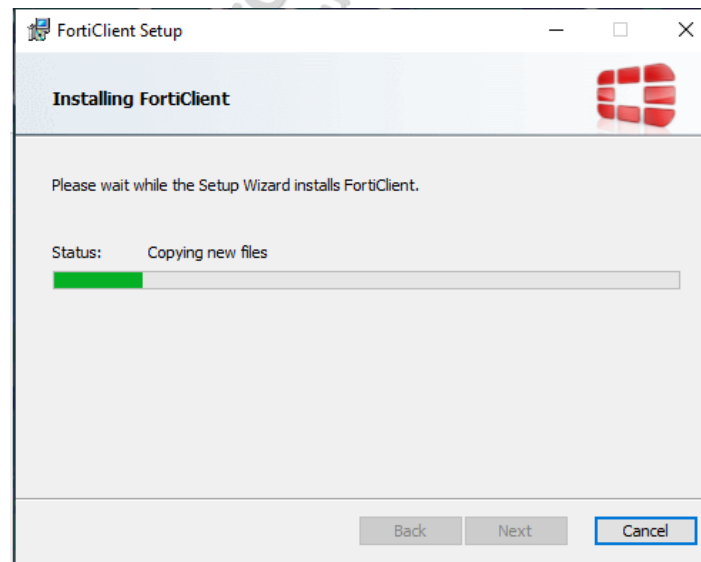
"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRS115



Descarga de los componentes de FortiClient.

Ejemplo: instalación




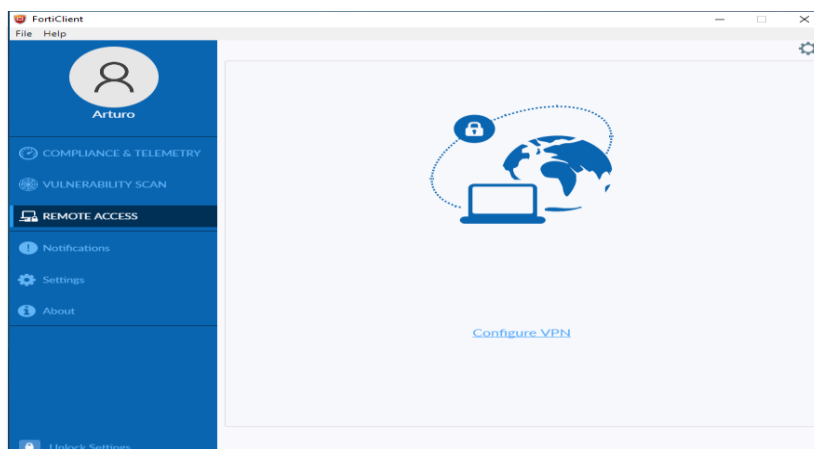
Ingreso a la aplicación y selección Remote Access en configure VPN.

Ejemplo: Aplicación Instalada

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 6 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15



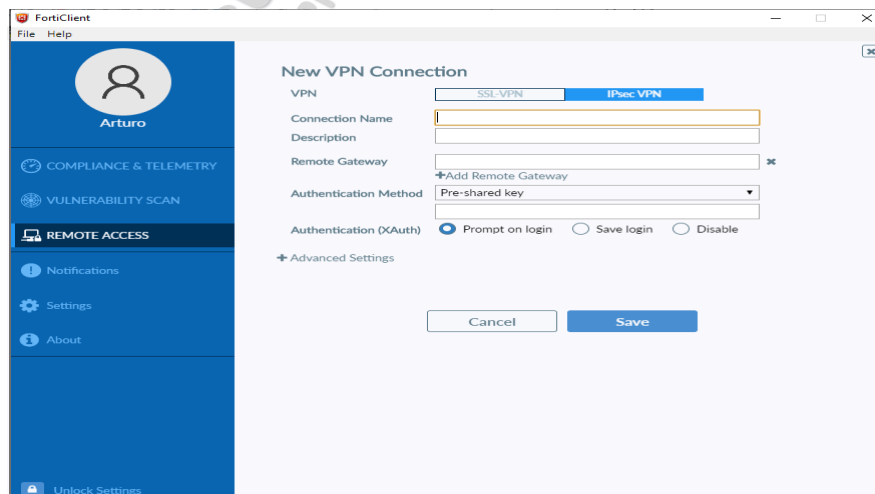
Se selecciona pestaña de IPSEC VPN.

Se crean los datos de conexión como el nombre de conexión **VPN 724** y en casilla descripción se debe agregar **724**.

REMOTE GATEWAY: Se ingresa la dirección IP o dirección WEB, se agrega el método de autorización como: PRE-SHARED KEY

Se agrega la llave pre-compartida posteriormente configurada en el FortiGate, selección de Save login e ingresar nombre de usuario que se preconfiguro previamente en el fortigate.
Save (guardar).

Ejemplo: Ingreso




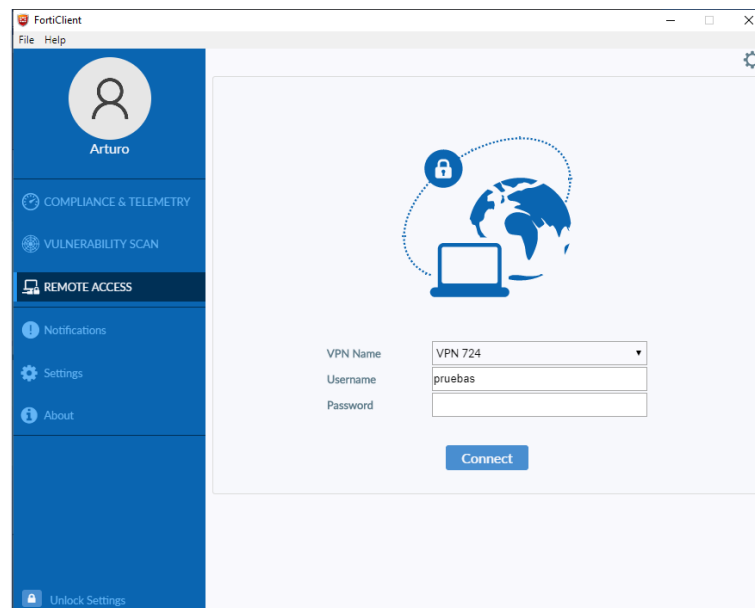
Retorno a la página de Login e ingresar la contraseña del usuario de la VPN, conectar.

Ejemplo: Conexión

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 7 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15



Procede a intentar de la conexión, ya conectado marcara el tiempo de conexión.

Se marca casilla de guardar contraseña.

Se vuelve a ingresar la contraseña y da opción de conectar.

6.3 Cifrado de la Wi-Fi


Todos los equipos que proporcionen acceso mediante wifi a la empresa deberán contar con el estándar de cifrado más seguro, actualmente WPA2.

Se siguen los siguientes pasos para cifrados de Wi-Fi siendo el responsable el Administrador de Infraestructura.

ACTIVIDAD	DESCRIPCIÓN DE ACTIVIDAD	REGISTRO
Cambio de contraseña Wi-Fi y acceso a modem	Acceso a Modem por medio de IP, ingresar usuario y contraseña, se dirige apartado de usuarios, se hace cambio de contraseña Usuario Administrador. Se dirige a apartado de WiFi y cambia contraseña WPA.	Se realiza el cambio de la contraseña conforme el Calendario de Revisión y Actualización del manejo de la información PECSRI15_F01(2) .
Deshabilitar SSID y Deshabilita WiFi	Selecciona apartado de WiFi la deshabilitación para que no se muestre el nombre de la Red.	NA
Deshabilitar WPS	Se desmarca la casilla de WPS para evitar la conexión por medio del botón WPS.	NA
Anotación de los cambios de contraseña.	Se anexa número de sucursal, contraseña del modem y fecha de cambios en Formato FO-SIS-08 .	Anotación de los cambios en formato Registros de contraseñas WiFi PECSRI15_F02(2)

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 8 de 12
--	-----------------------	---------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

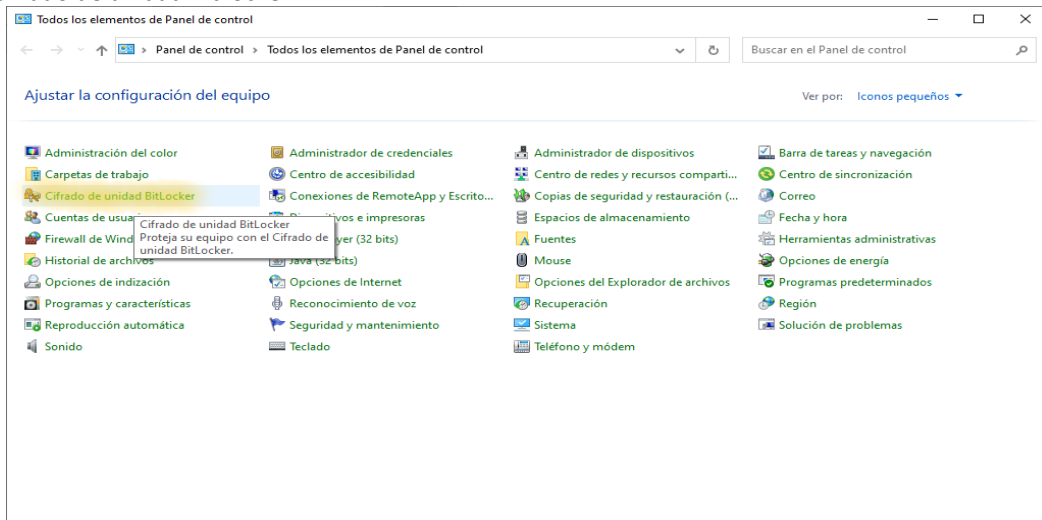
	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15

6.4 Cifrado de unidades

La operación del cifrado de unidades se ejecuta en todos los equipos, de forma inicial antes de que el equipo comience con las operaciones de la organización.

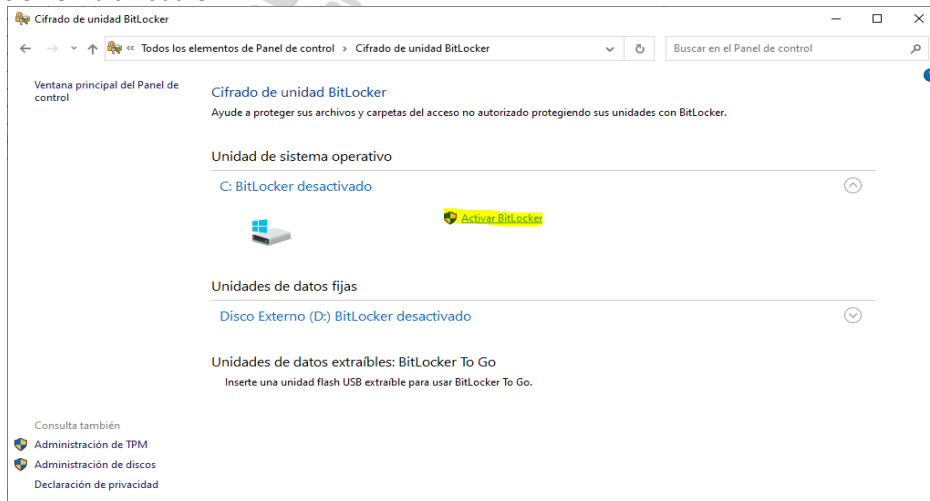
Ingresa a panel de control en opción cifrado de unidad BitLocker contenida en el sistema operativo de Windows 10, 7 y Server.

Ejemplo: Cifrado de unidad BitLocker



Se activa la opción de activación en la unidad C.


Ejemplo: Activación en la unidad C



En caso de tener problemas para desbloqueo de PC, el mismo sistema cuenta con un archivo que permite el desbloqueo del acceso a los archivos y carpetas.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 9 de 12
--	-----------------------	---------------------------

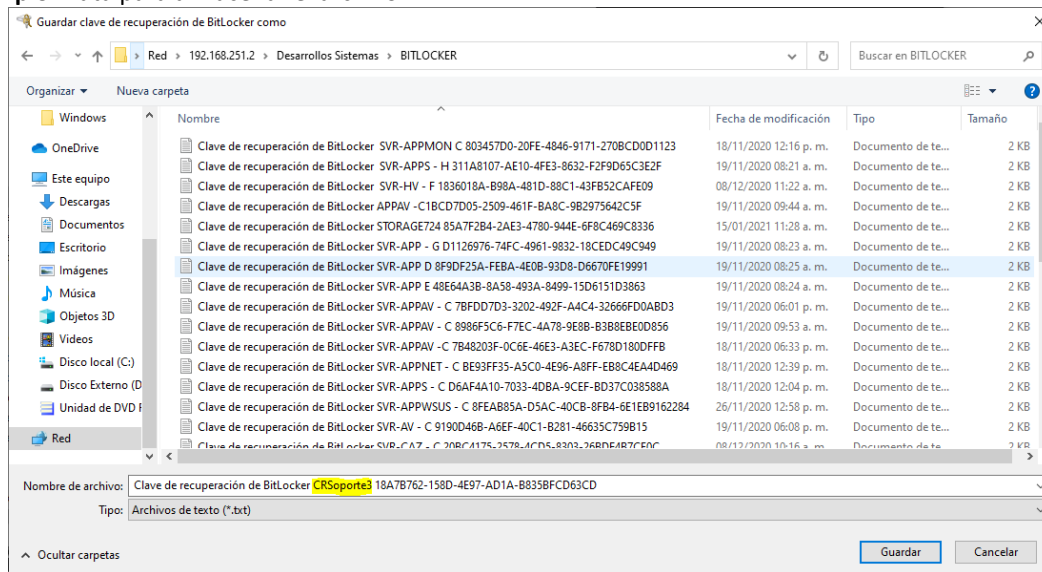
"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15

Solicitud de la ruta para almacenar el archivo:

Se guarda en carpeta Red:\\192.168.251.2\Desarrollos Sistemas\BITLOCKER

Ejemplo: Ruta para almacenar el archivo




Selección de nombre: Se utiliza el nombre del equipo que se asigna desde el funcionamiento de las operaciones de 724.

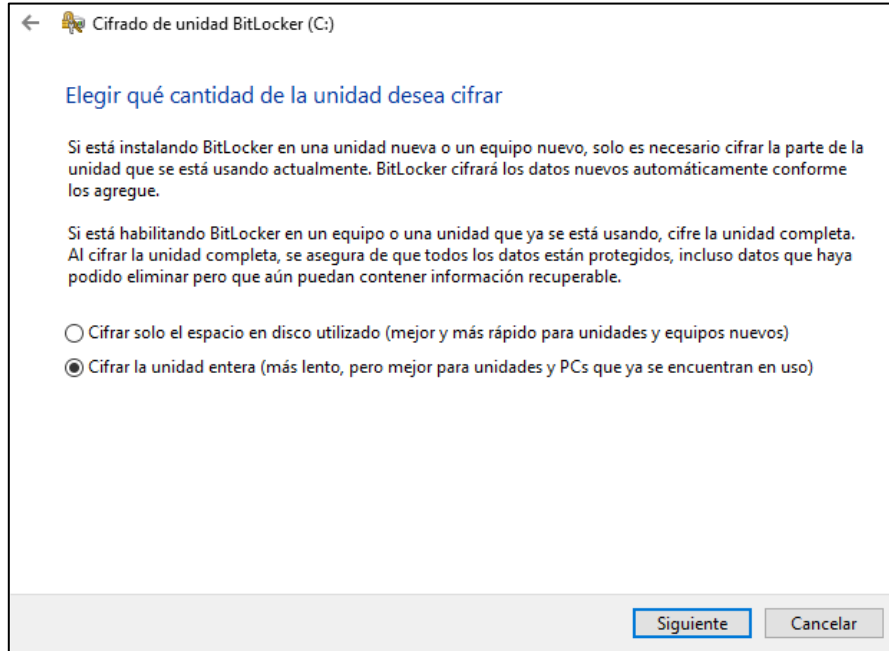
La propia configuración solicita la forma de cifrado si es que se requiere cifrar el disco duro completo o el espacio utilizado. Se considera el cifrado completo en la siguiente figura:

Ejemplo: Cifrado de la unidad BitLocker

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 10 de 12
--	-----------------------	----------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15



Este sería el modo de cifrado dependiendo si la unidad es fija/extraíble. Se verifica si las unidades se realizaran cifrados datos y se selecciona la casilla de ejecución de sistema de BitLocker.

El equipo se reinicia, se muestra el porcentaje de cifrado.

Finalización del cifrado.

Validación de cifrado.

Se realiza una copia de seguridad de la clave de recuperación. Para los casos de que el equipo cuente con más de un disco duro se realiza y activa el bitLocker del disco Duro externo.

Nota 1: El responsable de la ejecución cifrado de unidades es el Administrador de Infraestructura y Auxiliar de Sistemas

Nota 2: Período de ejecución de cifrado de datos: Anual

6.5 Números de Identificación Personal y contraseñas

Todos los ID's de usuario y contraseñas utilizadas para proteger las llaves de cifrado deben cumplir con los requisitos de complejidad y longitud, esto se considera en la **Gestión de Contraseñas PECRRH10**.


6.6 Resguardo de Llaves

6.6.1 Resguardo de llaves para conexión al exterior con la VPN

Almacenamiento de las llaves que se generan en el FortiClient, es un formato propio que el administrador de infraestructura y auxiliar de sistemas tienen la responsabilidad de instalar y habilitar los canales de

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 11 de 12
--	-----------------------	----------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento Especifico
	Título:	Cifrado de datos y Resguardo de llaves
	Código:	PECRSI15

conexión exteriores hacia la red de la organización deberán ser registradas en formato **Llaves Pre-compartidas VPN PECRSI15_F03(2)**.

Todas las claves/llaves de cifrado emitidas por la Organización se deberán proteger para evitar la divulgación o mal uso de terceros que atenten con la protección de información, ver **Política de Resguardo de llaves (PECRSI15_PO02(3))**

6.7 Pérdida y Robo

La pérdida, robo o posible divulgación no autorizada de cualquier llave/clave de cifrado cubierto por esta política debe de ser reportado inmediatamente al equipo de Sistemas IT de Comercializadora rápido S.A. de C.V.

7. DIAGRAMA DE FLUJO

Puesto involucrado	Puesto involucrado	Puesto involucrado	Puesto involucrado
NA	NA	NA	NA

8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI15_F01(2)	Calendario de Revisión y Actualización del manejo de la información
	PECRSI15_F02(2)	Registros de contraseñas WiFi
	PECRSI15_F03(2)	Llaves Pre-compartidas VPN
Ayuda visual	NA	NA
	PECRSI15_PO01(3)	Políticas de cifrados de datos
Políticas	PECRSI15_PO02(3)	Política de Resguardo de llaves
	PECRRH10	Gestión de Contraseñas
Otros (documento externo)		

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 12 de 12
--	-----------------------	----------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"