POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN (PESI)

ANTECEDENTES:

Este documento pretende ser una Guía de Políticas Específicas, para los temas de Seguridad de la Información, que serán abordados a continuación.
Estas Políticas deben ser aprobadas por el Directorio, y enviadas a todo el personal, proveedores, contratistas, colaboradores externos, y toda persona o empresa que mantenga contacto con Corporación Vial del Uruguay S.A (en adelante CVU).

A.5.1.1 Políticas para la seguridad de la información.
Contamos con una política integrada aprobada de calidad, medio ambiente y seguridad y salud. Asimismo, contamos con el presente documento, que especifica todas las políticas de Seguridad de manera específica, así como una Declaración de Aplicabilidad (en adelante DdA, documento Declaración de Aplicabilidad PCI_V3)

A.5.1.2 Revisión de las políticas de Seguridad de la Información.
A.6.1.1 Roles y responsabilidades de la Seguridad de la Información.
PCI-DSS 12.1.1 Revisión de las políticas de seguridad.
PCI-DSS 12.4 Responsabilidades de Seguridad de la Información.
PCI-DSS 12.5 Asignar a una persona o equipo las responsabilidades de establecer, documentar y distribuir políticas y procedimientos de Seguridad de la Información. Supervisar y analizar alertas de Seguridad de la Información.
PCI-DSS 12.6.2 Distribución de la política de Seguridad de la Información y confirmación de lectura.
Para cumplir con estas actividades, Corporación Vial ha creado y designado, un Comité de Seguridad de la Información.
Este Comité sesiona a demanda o ante cambios significativos, revisando los aspectos de las PESI, así como también aspectos del SGI en general.
CVU realiza de forma anual, o ante cambios significativos la distribución a todo el personal, y a los proveedores externos, de las políticas y procedimientos, de manera que estén al tanto de todos estos y se realicen las tareas conforme fue establecido.
CVU guarda registro de lectura correspondiente para el personal interno.
Esto está incluido como información de entrada en la Revisión por la Dirección, así como la DdA.
El comité define las políticas, realiza la revisión de las mismas, y planifica aspectos a cambiar o mejorar.
Queda registro de las versiones anteriores de Políticas de Seguridad Específicas a modo de consulta, cambiando el número de versión ante un cambio.

Las principales actividades a desarrollar del Comité de Seguridad de la Información son:

- Realizar el estudio de la Política de SI, previo a su aprobación.
- Proponer las responsabilidades generales en materia de SI.
- Brindar lineamientos estratégicos al OSI.

- Apoyar y aprobar aquellas iniciativas que incrementen la SI.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Promover la difusión y apoyo a la SI dentro de las áreas.

El mismo se encuentra integrado por:

- Gerente General
- Gerente de Control Económico Financiero
- Oficial de Seguridad (OSI)
- Analista Supervisor de Contrataciones
- Analista Jefe del CCO
- Analista de Software del CCO
- Analista de Hardware del CCO
- Coordinador de SGI
- Delegado de Protección de Datos Personales ante la URCDP

- **Responsable en Seguridad de la Información (Analista Jefe del CCO)**

Principales Actividades

- Definición, actualización y mantenimiento de los activos de información y asociados.
- Análisis de riesgos de SI con base a los establecidos en el Sistema de Gestión de la SI.
- Definición del plan del tratamiento de riesgos de SI.
- Ejecución del plan de tratamiento de los riesgos de SI.
- Definición y generación de métricas de SI.
- Identificar cambios significativos en las amenazas y la exposición de la información.

- **Responsable en Seguridad Física (Analista de Hardware del CCO)**

Principales Actividades

- Implementar las medidas de control de seguridad de acceso físico a las instalaciones de CVU y al Datacenter, gestionando los niveles de permisos.
- Asegurar el acceso no autorizado a los servidores instalados en los puestos de peaje.
- Realizar inspecciones periódicas para asegurarse que se mantienen las medidas de protección definidas en el SGI.
- Informar a la jefatura del CCO sobre el funcionamiento de las medidas implementadas.
- Medir la efectividad de los planes de contingencia, en base a los resultados de los simulacros. Recomendar los pasos a seguir en caso de que fallen las medidas de protección.

- **Oficial de Seguridad de la Información (OSI)**

Se trata de una figura cuya labor es garantizar la implementación de políticas, medidas y acciones, que contribuyen a la salvaguarda de la información de la organización, en los contextos que sean pertinentes según sea ésta pública o confidencial.

Principales Actividades

- Verificar la alineación de la seguridad de la información (SI) con los objetivos de la organización

- Implementar y documentar el Sistema de Gestión de Seguridad de la organización.
- Revisar en forma periódica los documentos y controles del Sistema de Gestión de SI de la organización.
- Coordinar con los "responsables" de los procesos y activos de información, la alineación con la seguridad de la información definida por la organización.
- Asegurar que la implementación de los controles de seguridad de la información es coordinada en toda la organización.
- Verificar la falta o superposición de controles en SI.
- Promover la difusión, concientización, educación y la formación en relación con aspectos de SI.
- Promover el cumplimento con la normativa y legislación vigente en relación con aspectos de SI
- Promover el cumplimiento de las políticas y documentos relacionados del Sistema de Gestión de la SI.
- Monitorear y analizar alertas, en caso de que amerite tomar alguna acción, deberá asignar cada caso al responsable del área/proceso involucrado.
- Evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad de la SI y las acciones recomendadas en respuesta a los mismos.
- Colaborar con los equipos responsables por la Gestión de Incidentes, del Riesgos y por la definición e implementación del Plan de Continuidad del Negocio.

- **Delegado de Protección de Datos Personales ante la URCDP**

Principales Actividades

- Asesorar en la formulación, diseño y aplicación de políticas de Protección de Datos Personales, para aquellas actividades que impliquen tratamiento de datos personales.
- Supervisar el cumplimiento de la normativa vigente en la materia.
- Proponer las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales.

A.6.1.2 Segregación de funciones.

Existen perfiles de cargo con tareas y responsabilidades asignadas.
Estos perfiles están disponibles en R.R.H.H.
Asimismo, están definidos estos perfiles a nivel de dominio, brindado acceso a lo necesario por cargo.
También existe una segregación de Red a nivel de vLAN's donde cada equipo puede acceder únicamente a los servicios que le corresponden al cargo.

A.6.1.5 Seguridad de la información en la seguridad del proyecto.

A.6.2.1 Política de dispositivos móviles.

LOS NOTEBOOKS propiedad de CVU que estén asignados a funcionarios para el desarrollo de sus actividades deberán tener las siguientes Características:

- Discos Duros Cifrados: Los discos duros de estos dispositivos estarán cifrados con la finalidad de evitar la pérdida o uso indebido de información, ante extravío, o robo de los Notebooks.
Para ello CVU ha definido e instalado el Software BITLOCKER o CRYHOD.
- Antimalware actualizado: Corporación Vial cuenta con licenciamiento para todos sus equipos de ESET ENDPOINT ANTIVIRUS. El mismo está configurado para actualizarse automáticamente contra el Servidor SRV-WSUS-WIN el cuál distribuye las actualizaciones del antimalware. Existe un escaneo rutinario programado semanal que analiza todo el equipo distribuido también por políticas de Consola Central.
- Los equipos deberán bloquearse automáticamente según lo definido en el punto de equipo desatendido.
- El registro del equipo y su asignación se encuentran en el documento **INVENTARIO_CVU_V2.**

LOS TELÉFONOS CELULARES propiedad de CVU que estén asignados a funcionarios para el desarrollo de sus actividades, deberán tener las siguientes características:
- Deberán contar con al menos un bloqueo de pantalla que sea activable a través de PIN, Huella Digital, o Patrón de Desbloqueo.
- A su vez deberán tener activado el bloqueo de Tarjeta SIM, de manera que la clave de la Tarjeta sea solicitada cada vez que se inicia el teléfono.
- El registro de estas características está en el Software Mobile Device Manager. IN-TI-720

Documento Vinculado	Ruta de acceso al Documento
RE-GI-720 + Nombre de Equipo.docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-720
RE-GI-717 – Control Dispositivos Móviles + Nombre usuario asignado	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-717
IN-TI-720 Mobile Device Management V1 .docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\TI\IN-TI-720

A.6.2.2 Trabajo remoto o teletrabajo.

Por el tipo de actividad que desarrolla CVU, y atendiendo los requisitos para la "Operación Continua", CVU brinda a sus funcionarios, operadores de Peaje y proveedores de servicio de mantenimiento, el servicio de Trabajo Remoto o Teletrabajo.
Todas las personas, que sean usuarias de este servicio, deberán registrarse en el Documento **RE-TI-705** para obtener un Usuario de Acceso Remoto con su respectiva clave.
Asimismo, se les entregará un TOKEN de Software (FORTITOKEN) lo que incrementa la seguridad brindando "doble factor de autenticación" (2FA).
A su vez, el Fortigate tiene cargado un certificado emitido por una CA válida uruguaya (avalada por UCE) que garantiza la autenticidad del servidor al que nos estamos conectando.
El Firewall de CVU es FORTINET, y los usuarios serán registrados en el TUNNEL SSL, para obtener ingreso a los Sistemas.
Los permisos a los sistemas que podrán ingresar son exactamente los mismos, que los brindados para sus usuarios de Red y usuarios de Sistemas.
Otro requisito es que los equipos que se conecten por VPN al Túnel de CVU, deberán contar con antivirus actualizado. Esto será responsabilidad del usuario que ingrese a CVU.

El Software homologado para estos ingresos a la red de CVU, es el FORTICLIENT, y no habrá otro método de ingreso.
Todos aquellos usuarios que "no cumplan" los requisitos aquí expresados o hagan un "mal uso" de esta herramienta, serán pasibles de la revocación de sus derechos de acceso remoto.
Para el acceso de proveedores, la conexión por defecto está cerrada, y se habilita contra solicitud por correo electrónico al OSI, quien habilita por defecto durante 24 hs la conexión del usuario, pudiéndose otorgar más tiempo para tareas de larga data.

A.8.2.1 Clasificación de la información.
A.8.2.2 Etiquetado de la información.
A.8.2.3 Manejo de activos.
Corporación Vial del Uruguay S.A. es una empresa que trabaja para el estado, y tanto la información de contratos, tránsitos, recaudación, etc, no solo es pública, sino que se encuentra publicada en los sitios Web de CVU y de Telepeaje.
En caso de que el Directorio de la Empresa defina como Información Clasificada, algún tipo de documento, el mismo deberá contar con una "marca de agua" con la palabra "confidencial". Para ello contamos con un formato preestablecido que está en poder de todos los funcionarios de la empresa. El mismo se llama FORMATO DOCUMENTO CONFIDENCIAL VACIO.DOCX
Las bases de datos de usuarios, proveedores, contratistas, que puedan llegar a tener información alcanzada por el "tratamiento de datos personales" se encuentra bajo la protección de Sistemas Gestores de Bases de Datos relacionales, a las cuáles SÓLO pueden acceder los usuarios que la necesitan, y los mismos cuentan con los perfiles adecuados.
Asimismo, la estructura de permisos de los "archivos de usuario" está protegida a nivel de Active Directory con las especificaciones de acceso que cada JEFE determina para su personal en los correspondientes perfiles.
Además, cada área de la empresa define un subgrupo de información "sensible" y un grupo de información "pública" para cada equipo de trabajo.
En un tercer nivel, se encuentra una carpeta "PUBLICA" disponible para todos los funcionarios de la empresa.
Corporación Vial solo muestra a sus funcionarios la información necesaria para realizar las tareas.

A.8.3.1 Gestión de los medios removibles.
Corporación tiene configurados todos los Antimalware Corporativos, de manera que cada vez que se detecte un Medio Removible, ya sea Pen Drive, Compactera USB, Disco Duro Externo, etc, el mismo antimalware dispara el escaneo de software malicioso del nuevo dispositivo detectado.
Esto se define por política en la consola de ESET PROTECT, y se traslada a todos los Endpoint de manera que esta medida no escape a ninguno de los usuarios. La misma solo puede ser modificada por Perfiles del Datacenter.

PCI-DSS 9.8.2 Destrucción de medios electrónicos.
A.8.3.2 Eliminación de medios.
A.11.2.7 Seguridad en la reutilización o descarte de equipos.
Cada vez que se deseche Hardware que cuente con información, ej. Pen Drives, Discos Duros, PC's, Notebooks, etc. los mismos deben ser o Formateados a bajo nivel o Destruidos. Se debe dejar evidencia del proceso realizado para destruir la información contenida en estos elementos.

Si la unidad es reutilizable, ej Discos Duros de Servidores/PC/Notebook, Pen Drives, Discos Duros Externos, los mismos serán formateados garantizando la total eliminación de la información.
En el caso de que no sean reutilizables, se deberá proceder a la destrucción del medio, garantizando su rotura o inutilización.
Es estos casos de destrucción física, se deberá dejar registro de la destrucción en la planilla: **RE-TI-709.**
Toda destrucción se realizará ante alguna jerarquía que testifique la misma, y se deberá dejar constancia firmada.

Documento Vinculado	Ruta de acceso al Documento
RE-TI-709. Destrucción de Medios con Informacion.xlsx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\RE-TI-709. Destrucción de Medios con Informacion.xlsx

A.9.1.2 Acceso a las redes y a los servicios de red.
A.9.3.1 Uso de información de autenticación secreta.
PCI-DSS 12.5.4
PCI-DSS 12.5.5
Existe un Procedimiento de Control de Acceso Lógico a los Sistemas, validado por el Comité de Seguridad.
El mismo hace referencia a los Accesos Lógicos, derechos sobre carpetas controlados por perfiles y registro de los mismos.
Están detallados en el Documento:
RE-TI-705.
A su vez los procedimientos para Altas de Usuarios a los Sistemas, están detallados en el Documento:
IN-TI-709 ABM USUARIOS WINDOWS-SISTEMA PEAJES V1_.docx
El registro de los usuarios del Sistema de Recaudación de Peajes, además queda en la Tabla de Auditoría del Sistema de Recaudación.

Documento Vinculado	Ruta de acceso al Documento
RE-TI-705 + nombre de usuario.docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\TI\RE-TI-705
IN-TI-709.docx ABM Usuarios Windows-Sistema Peajes V1_	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-709

CVU realiza monitoreos continuos a través de nuestro SIEM (GRAYLOG) de accesos a todos los sistemas, en especial a aquellos con información de datos de tarjeta de crédito.

A.9.4.2 Procedimientos de inicio de sesión seguros.
Todos los Sistemas de CVU, cuentan con pantalla de Login, con su correspondiente usuario-clave, para acceder a los mismos.
No existe un solo sistema en CVU, que no requiera un inicio de sesión a través de estos parámetros.
ACCESOS VPN: Cuentan con Login de doble autenticación. Además del usuario y la clave, se debe contar con un TOKEN de Fortinet, para poder acceder. "Doble Autenticación". También existe un certificado de autenticación de la VPN, que valida "vpn.cvu.com.uy".

ACCESOS A LA RED: Todos los usuarios de los dominios están registrados con su perfil. No es posible ingresar a la Red de CVU, sin usuario-clave.
ACCESOS A SISTEMAS: Todos los usuarios que necesiten entrar a un sistema específico de la empresa, deben primero ingresar al dominio con su usuario y su clave. Una vez registrados dentro del dominio, pueden acceder al sistema específico que necesiten, pero tendrán que utilizar su conjunto de usuario-clave, para cada sistema específico que necesiten acceder.

A.9.4.3 Sistema de gestión de contraseñas.
A.10.1.2 Gestión de claves.
A.11.2.8 Equipo de usuario desatendido.
PCI-DSS 8.1.8 Cierres de sesión automáticos.
PCI-DSS 8.2.2 Verificación de identidad ante cambio de contraseñas.
PCI-DSS 8.2.6 Cambio de clave obligatorio luego de un reinicio de clave.
PCI-DSS 8.3.1 Autenticación MultiFactor.
PCI-DSS 8.4 Guías de uso de contraseñas.
PCI-DSS 8.5.1 Requerimientos adicionales para prestadores de servicio.
PCI-DSS 8.6 Uso de mecanismos de autenticación adicionales.
PCI-DSS 8.7 Acceso a base de datos.
PCI-DSS 12.3.8 Desconexión automática de sesiones.
PCI-DSS 12.3.9 Activación de accesos remotos para proveedores con desactivación automática después de su uso.

CVU cuenta con políticas de contraseñas.
Los accesos a la red de CVU son controlados por políticas de grupo de dominio, la cual tiene establecida todas las restricciones y características de "buenas prácticas" (detalladas a continuación).
Los Dominios de CVUNET y PEAJES cuentan con las políticas de grupo activas para los siguientes Ítems.

- Largo mínimo de 7 caracteres.
- Deben cumplir con los requerimientos de Seguridad de AD.
- No se pueden repetir contraseñas usadas previamente. Guardamos 5 contraseñas.
- Las contraseñas caducan cada 90 días.
- Los accesos para SQL no pueden ser mixtos. Únicamente con el usuario de SQL.
- Las cuentas de Active Directory, NO SIRVEN para acceder al Sistema de Base de Datos. Cada usuario que necesite ingresar a la misma, deberá contar con una clave previamente autorizada con el perfil que corresponda.
- Las únicas cuentas que acceden al Motor de Base de Datos, son las de los DBA.
  - Personal de la Empresa que desarrolla el Sistema de Recaudación.
  - Jefe del Centro de Consolidación de Operaciones.
  - Analista de Hardware.
  - Analista de Software.
- Las cuentas de dominio, se cierran y exigen contraseña nuevamente luego de 10 minutos de inactividad. Esto está definido por políticas de dominio.
- El Sistema de Recaudación (Sistema que accede a los datos) utiliza para todas sus operaciones, STORED PROCEDURES almacenados en la base de datos y los mismos están encriptados.

- A excepción de los DBA y los Proveedores de Servicio de Desarrollo y Mantenimiento del Sistema de Recaudación, no existen accesos o cuentas para ingresar a los mismos.
- Los accesos al sistema de recaudación (ambiente PCI) requieren además que los de AD cuenten con las siguientes características.
  - Largo mínimo 8 caracteres.
  - Se vencen cada 120 días.
  - No se pueden repetir más de 2 caracteres de la última contraseña.

GUÍA PARA CLAVES SEGURAS:

- No divulgue sus claves de acceso, ni de forma verbal ni escrita.
- Se necesitan usar Números, Letras, Mayúsculas, Minúsculas y Caracteres especiales para los accesos de Windows.
- Windows recuerda sus últimas 5 contraseñas y ninguna de ellas podrá ser reutilizada en ese período.
- Si sospecha que su clave fue comprometida, solicite o cambie la clave de manera inmediata.
- Cada vez que un Administrador reinicie su clave, el sistema le solicitará que la cambie al siguiente acceso.

Los usuarios deberán estar todos nominados. No se aprobarán cuentas genéricas de ningún tipo, salvo que el sistema así lo requiera.
Cada sistema contará con una cuenta distinta. La misma cuenta no sirve para entrar a 2 sistemas diferentes.
Aunque el proveedor de servicios mantenga diferentes personas atendiendo los sistemas, cada uno de ellos deberá contar con su propia cuenta, no estando permitido compartir la cuenta entre varios funcionarios del prestador de servicios.

Para los accesos remotos por VPN, cada usuario contará además de su cuenta y su clave de FORTINET, con un FORTITOKEN de software. Además, los Firewalls de CVU cuentan con un Certificado de autenticidad emitido por una CA autorizada por UCE.

PCI-DSS 8.1.4 Eliminar/Deshabilitar cuentas de usuario inactivas.
El OSI cuenta con una tarea de revisión de usuarios inactivos en los sistemas críticos de CVU (AD, Sistema de recaudación, Correo electrónico, entre otros).

PCI-DSS 8.1.5 Gestión de ID de terceros
Se cuentan con 2 proveedores críticos, AT y TELSIS. TELSIS necesita acceso 24/7 por temas de requerimientos del negocio y contratos.

A.9.4.4 Uso de programas utilitarios privilegiados.
A.12.5.1 Instalación de software en sistemas operacionales.
A.12.6.2 Restricciones sobre la instalación de software.
PCI-DSS 12.3.7 Lista de software aprobado por la empresa.
La instalación de cualquier tipo de Sistema Operativo, Software, Drivers, Configuraciones de acceso, unión de equipos a los Dominios, o cualquier configuración que implique cambios en los equipos, es realizada por personal del Centro de Consolidación de Operaciones. Los usuarios que

no pertenecen a este equipo, no pueden cambiar, instalar o modificar instalaciones de estos elementos sin una clave que los autorice.

Se cuenta con un listado maestro de los Softwares que se pueden instalar por parte de personal del Datacenter en los equipos clientes.
El mismo es revisado y actualizado de manera continua.
Es una guía y un control del software que "puede" llegar a estar instalado en los equipos cliente de CVU.

Documento Vinculado	Ruta de acceso al Documento
RE-TI-727 - EQUIPAMIENTO MINIMO.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Equipamiento Minimo.docx
RE-TI-712 – INVENTARIO SOFTWARE PERMITIDO	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\RE-TI-712 – INVENTARIO SOFTWARE PERMITIDO.xlsx

A.9.4.5 *Control de acceso al código fuente de los programas.*
PCI-DSS 6 Desarrollar y mantener sistemas y aplicaciones seguras.
Como cualquier área de CVU, los códigos fuente de programas que se desarrollan de manera interna, están sometidos al mismo sistema de permisos que el resto de la información.
Solo los Administradores del Dominio, tienen acceso al código fuente de los programas desarrollados por CVU.

Todos los lineamientos vinculados al área de desarrollo están en el siguiente documento:

Documento Vinculado	Ruta de acceso al Documento
PR-GR-708 Desarrollo Seguro de Software	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\

A.10.1.1 Política sobre el uso de controles criptográficos.
A.13.2.1 Política y procedimiento de transferencia de información.
A.13.2.3 Mensajería electrónica.
A.18.1.5 Regulación de los controles criptográficos.
PCI-DSS 4.2 Transmisión segura de PAN's.
PCI-DSS 4.3 Comunicación de procedimientos.
El Sistema de Recaudación de Peajes cuenta con un Sistema de encriptación, a través del cual todos los datos sensibles como ser claves, información de crédito de usuarios, quedan dentro del Sistema de Gestión de Bases de Datos Relacionales (SQL Server) grabados y protegidos bajo este algoritmo, que no es conocido por el personal de la CVU. Es manejado exclusivamente por el proveedor del Sistema de Recaudación. (TELSIS).
Únicamente permiten conexiones cifradas, utilizando para ello protocolos de cifrado TLSv1.2 o superior, a su vez, todos los certificados utilizados deben ser emitidos por una entidad de confianza.
No se podrán enviar bajo ningún concepto, números PAN de Tarjetas de Créditos por correo electrónico o ningún otro medio que no sea el servicio específicamente dedicado para esto.

A nivel de tráfico de archivos de pasadas de tránsito pospagos, los mismos son depositados en un SFTP (SYNCPLIFY.ME), salvo los que son depositados en sitios de los Sellos, donde se requiere usuario, contraseña y los mismos cuentan con Certificados.
Este servicio utiliza un canal seguro SFTP que restringe el acceso únicamente desde las IP de origen autorizadas.

No se reciben o envían archivos abiertos por correo, o que no sean en sitios publicados por los sellos para tales fines, con toda la seguridad embebida que estos contienen.

Firmas digitales avanzadas, se aplica el uso de algoritmos de cifrado como herramienta de control, protección de la confidencialidad, autenticidad o integridad de la información. Esta política aplica tanto al directorio de CVU como a su gerente general. Mediante Token físicos se realizan firmado de correo electrónico (cuando se requiere), operaciones en diferentes bancos de plaza, presentación de documentación ante BCU y firmado de documentos digitales. Es responsabilidad de cada usuario proteger y salvaguardar su dispositivo de cifrado, como así también las claves relacionadas.

A.9.1.1 Política de control de acceso.
A.11.1.1 Perímetro de seguridad física.
PCI-DSS 7 Restringir el acceso físico a los datos del titular de la tarjeta.
PCI-DSS 9.1 Controles de acceso.
PCI-DSS 9.3 Controle el acceso físico de los empleados a las áreas confidenciales de la siguiente manera:
• El acceso debe estar autorizado y basarse en la función de cada persona.
• El acceso debe cancelarse inmediatamente después de finalizar el trabajo, y todos los mecanismos de acceso físico, como claves, tarjetas de acceso, deben devolverse o desactivarse.

Existe un Procedimiento de Control de Acceso, validado por el Comité de Seguridad.
El mismo hace referencia a los Accesos Físicos al Edificio de la CND, como también a las oficinas de CVU en el 5to piso. En el mismo se especifican además los controles específicos para acceder al DataCenter de CVU.

CVU cuenta con los siguientes accesos:

1. Acceso a Telepeaje
2. Acceso a compras y contrataciones
3. Acceso a Directorio

Estos 3 accesos están protegidos por Sensores Biométricos, al cual solo tienen acceso, las personas habilitadas para acceder a las oficinas, los días y horarios establecidos.

A su vez existe un acceso interno que divide el Centro de Consolidación de Operaciones con Compras y Contrataciones, y otro con que divide el Centro de Consolidación de Operaciones con el acceso al Directorio. Estos 2 accesos también están protegidos por dispositivos biométricos con los mismos accesos que los externos.

El Datacenter de la empresa, cuenta con otra área de seguridad, protegida por una puerta de vidrio que también cuenta con Sensor Biométrico, al cual solo tienen acceso las personas que trabajan en el Centro de Consolidación de Operaciones (CCO).
Este control Biométrico guarda todas las aperturas de puertas generadas, manteniendo la fecha, hora, que puerta se abrió y quien la abrió.
CVU cuenta con el historial completo desde que se instaló el Sistema

Se utiliza un circuito cerrado de videovigilancia en las oficinas de CND, CVU. Se mantienen respaldo de las grabaciones por al menos 3 meses.

En el área del Operaciones del Centro de Consolidación de Operaciones (CCO) si bien no se encuentran los Servidores o Storages con información, al acceder a los datos de los usuarios (alcanzado por la Ley de Protección de Datos Personales de AGESIC) no se recibe público. Cuando en raras ocasiones necesitamos atender público, el mismo es atendido en la Recepción interna de CVU.
Todos estos procedimientos se encuentran detallados en los Documentos:

Documento Vinculado	Ruta de acceso al Documento
IN-TI-703 Control de Acceso Físico al Edificio CND V2.docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-703
IN-TI-700 ABM Control de Acceso Físico a CVU V2.docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-700

CVU no permite conexiones en áreas públicas. No permiten el uso de wifi. La única red wifi disponible es propiedad de CND.
Las conexiones a las diferentes bocas de red están identificadas, no permitiéndose la conexión de dispositivos sin la aprobación del encargado de infraestructura.

Todas las bocas de red se encuentran debidamente documentadas en la siguiente planilla:

Documento Vinculado	Ruta de acceso al Documento
Infra CVU.xlsx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\

Todas las bocas de red de la oficina acceden únicamente a las VLAN de usuarios de peajes y de usuarios de CVU. Todas las IP son fijas, las VLANS no tienen acceso a ningún servidor. Todas las conexiones a las diferentes VLANS son controladas por el Firewall interno quien deniega la conexión.

Únicamente las IP's de los Administradores de CVU cuentan con permisos de acceso a la totalidad de las VLANS. Esto es controlado por el firewall interno el cual tiene una regla específica para este acceso.

A.9.1.1 Política de control de acceso.

PCI-DSS 3 Proteger los datos almacenados del titular de la tarjeta.

CVU mantiene un estricto control trimestral sobre los datos de tarjetas de créditos para asegurarse que estos no permanezcan en los sistemas de CVU por más tiempo que el definido en la relación comercial con el propietario de la misma.
Para eliminar archivos (enviados por las operadoras) almacenados en el ambiente controlado (vm), se procede a alterar manualmente la modificación mediante un script el contenido del archivo.

Aquellos titulares que ya no son clientes, se procede a eliminar en el sistema los datos relacionados a su tarjeta de crédito/débito.
No se utiliza ni guarda el código verificador de 3 cifras de las tarjetas. Solo se utiliza el número PAN, el cual es conservado junto al nombre del Titular y la fecha de Vencimiento de la tarjeta.
Los números PAN se almacenan en la base de datos del sistema TCP-TOLL de forma cifrada. Utiliza para ello una clave AES-256.

Se enmascara en la aplicación TCP-TOLL los primeros 12 dígitos mostrando SOLO los últimos 4. Se permite la visualización completa de los números PAN (por requerimientos del negocio y forma de intercambiar información con las operadoras de plaza) solo a un grupo reducido de empleados a través de accesos restringidos y debidamente autorizados.

Se cuenta con una infraestructura de clave pública (PKI) interna para la gestión de todas los certificados internos y el ciclo de vida está reflejado en el siguiente documento.

Documento Vinculado	Ruta de acceso al Documento
Manual CA.pdf	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\

A.11.2.9 Política de escritorio y pantalla limpios.

CVU explica y comunica a los usuarios en los talleres de Concientización, lo siguiente:

1. Dejar los monitores apagados o protegidos mediante un mecanismo de bloqueo de pantalla mediante contraseña.
2. Retirar de manera inmediata de las impresoras los documentos que contengan información sensible o clasificada.
3. Con respecto a los escritorios de trabajo físicos, se deben mantener los mismos ordenados con la documentación necesaria para trabajar. "No deben" existir bajo ningún concepto, papeles, postits, hojas, etc., con ningún tipo de información sensible, ya sea de nombres de usuarios, de contraseñas, datos personales, etc
4. Tener en cuenta las clasificaciones de la información contenida en las estaciones de trabajo y sus correspondientes riesgos para CVU.

Ante la verificación del incumplimiento de lo estipulado en este punto se debe:

- Identificar las causas.
- Evaluar acciones necesarias para el cumplimiento.
- Implementar las acciones correctivas necesarias

- La Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

A.12.1.1 Procedimiento de operación documentados.

Los Procedimientos de CVU para todas las áreas, están documentados en el Sistema de Gestión de Calidad.

Documento Vinculado	Ruta de acceso al Documento
RE-GI-400 – Listado Maestro de Documentos	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-400
CARPETA FISICA CON PROCEDIMIENTOS.	BIBLIORATOS EN PODER DEL COORDINADOR DEL SGI

A.12.1.2 Gestión de cambios.

CVU cuenta con Bitácora de seguimiento a sus Sistema de Recaudación.
El Centro de Consolidación de Operaciones cuenta con Bitácora de apuntes ante cambios en el Sistema de Recaudación.
A su vez, el Sistema de Gestión integrado, cuenta con una Matriz de Gestión del Cambio.

Documento Vinculado	Ruta de acceso al Documento
RE-TI-720 – BITACORA DE SISTEMA TCP-TOLL	M:\CCO\CCOS SENSIBLE\BITACORAS
MATRIZ DE GESTION DEL CAMBIO.docx	M:\SITEMAS DE GESTION\REGISTROS APROBADOS\GI\RE-GI-508

A.12.1.3 Gestión de la capacidad.

CVU cuenta entre sus Procesos, con el Presupuesto Anual para el siguiente año.
En este documento se evalúan tanto Hardware, Software, Equipamiento, Servicios, Contratos de Mantenimiento, y todas las necesidades que se vayan detectando, a través de las mediciones realizadas, y de los requerimientos que van surgiendo.
El mismo es entregado al Directorio en el Mes de Setiembre, y se pre-aprueban las compras para el año siguiente, con las que el Directorio esté de acuerdo.
A partir de allí, se pueden comenzar a realizar las compras pre acordadas, cumpliendo con todos los ítems del Procedimiento de compras aprobado en CVU.
Además, el Centro de Consolidación de Operaciones ha adquirido un sistema de Monitoreo de Hardware y Software (Nagios XI) licenciado para 200+ equipos donde se controlan los procesos y capacidades críticas.

Documento Vinculado	Ruta de acceso al Documento
PRESUPUESTO 2022.docx	PLANILLA DE BIENES DE USO – PLANILLA DE SERVICIOS
COMPRAS PRESUPUESTO 2022.	M:\BORRADORES\COMPRAS PRESUPUESTO\2021

A.12.2.1 Controles contra código malicioso.

PCI-DSS 5 Proteger los sistemas contra malware y actualización de sistemas y antivirus.

CVU cuenta con un Software Homologado a nivel Corporativo para todos sus equipos, tanto en la Oficina Central, como en los Peajes.
Se trata de una licencia bianual, para 160 equipos que están protegidos por este sistema.
El mismo es el ESET ENDPOINT ANTIVIRUS.

Trabaja a nivel de ambas redes de CVU. CVUNET y PEAJES.
Los equipos se actualizan de forma diaria mediante una consola centralizada, y la configuración de este Antivirus está protegida por clave, de manera que actualmente únicamente el personal de Datacenter y el Oficial de Seguridad pueden realizar cambios sobre esta consola.

Se cuenta con un deploy total de los equipos por GPO. El dominio de peajes tiene un total del 100% de los equipos instalados.
CVU implementó una consola centralizada (ESET PROTECT (Server), versión 9.0) con el fin de mantener las rutinas de control de todos los antivirus de forma centralizada. Dentro de dichas tareas se destacan las de actualización de firmas, escaneos programados, permisos de cambios y gestión de alertas en tiempo real.

Documento Vinculado	Ruta de acceso al Documento
IN-TI-719 ESET-PROTECT V1.docx	M:\SISTEMAS DE GESTION\PUBLICO\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-719

Dentro de sus principales características están:

- Detecta amenazas desconocidas y nuevas al utilizar 3 modelos diferentes de Machine Learning
- En la versión 9 de los productos para equipos Windows, implementamos una nueva función de seguridad que protege los dispositivos frente a los intentos de adivinar las credenciales y establecer una conexión remota. Puede configurar fácilmente esta función mediante una política directamente desde la consola y crear exclusiones desde la sección Detecciones cuando se bloquee un elemento que no deba bloquearse.
- Protección Anti-Ransomware y Anti-rootkits en tiempo real

El oficial de seguridad cuenta con una tarea de control dentro de Service Desk para verificar dicho punto.

Las tareas se llaman:

- Control Estado Antivirus
- Verificación vulnerabilidades en sistemas sin AV

Dentro de la consola se configura una tarea de escaneo programado llamada “escaneo semanal” con el perfil “SmartScan” para que se realice todos los martes a las 10 de la mañana.
Las firmas son descargadas de forma diaria cada 1 hora por el servidor SRV-WSUS-WIN dentro de la carpeta \\192.168.105.13\Eset_Srv_Updates para que todos los equipos de la red actualicen las firmas desde allí.
Luego la consola de ESET le indica a todos los clientes de forma diaria cada 1 hora que descarguen las firmas desde dicha ubicación remota.

Se cuenta con protección desde la consola para que salvo el personal de Datacenter o el Oficial de Seguridad, no puedan ingresar a las opciones avanzadas del antivirus. Solo el departamento de TI

tiene permisos para realizar modificaciones en los antivirus. El antivirus se encuentra protegido por contraseña en cada puesto de trabajo.
Protección en tiempo real activada desde la consola en todos los equipos.

Todos los equipos de Corporación Vial del Uruguay, son protegidos por un Antimalware Corporativo que CVU mantiene desde el año 2013.
El mismo es el ESET NOD 32.
En cada equipo nuevo se configura para que los usuarios no cuenten con permiso de inhabilitación, escaneo automático al insertar medios removibles, y que los usuarios no puedan cambiar ningún parámetro de la configuración.
Los equipos que se conectan a Internet, (Dominio CVUNET) son actualizados directamente contra Internet, mientras que los equipos de NO tienen salida a Internet (Dominio PEAJES) se actualizan contra un Directorio de Actualización.
Todo esto es de manera automática y programada.

A.12.3 Respaldo de la información.
PCI-DSS 9.5.1 Inspección de instalaciones.

CVU cuenta con un Procedimiento formal detallado de respaldos.
El Centro de Consolidación de Operaciones, realiza respaldos de la totalidad de su infraestructura de forma diaria.
A su vez, el Centro de Consolidación de Operaciones, también cuenta con un Procedimiento de Restauración, para garantizar que los respaldos no estén corruptos, o que estén dañados de alguna manera.

Documento Vinculado	Ruta de acceso al Documento
PR-GI-401 Procedimiento de Control de Registros V8	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\PROCEDIMIENTOS APROBADOS\PR-GI-400
RE-GI-402 Control de Restauraciones informáticas V2	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-402
RE-GI-706 Verificación de Respaldos + FECHA	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-706 **DOCUMENTOS COMPARTIDOS**
RE-GI-705 Registro de Respaldos V3	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\GI\RE-GI-705 **DOCUMENTOS COMPARTIDOS**

NOTA: Para dar cumplimiento al punto INSPECCIÓN DE INSTALACIONES, se designa al OSI de la empresa, para realizar una inspección anual, para verificar que las instalaciones donde se guardan los respaldos, están acordes a los puntos de protección, seguridad, mantenimiento, etc.

A.12.4.2 Protección de la información de registros.
PCI-DSS 10 Rastrear y monitorear todo el acceso a los recursos de la red y los datos del titular de la tarjeta.

CVU mantiene registros por un lapso de un año, en un concentrador de logs (Graylog), de las actividades llevadas en el Active Directory, Firewalls, Switches y en el PC tarjeta.
Las pistas de auditoría son accedidas únicamente por los integrantes del equipo de infraestructura, el OSI y el jefe del área de IT; las pistas de auditoría no se pueden modificar.

A.12.4.4 Sincronización de relojes.
PCI-DSS 10.4 Usar sincronización de tiempo.
PCI-DSS 10.4.3 Fuentes NTP.

Existen en CVU dos grandes dominios.
Tanto el Dominio CVUNET, el Dominio PEAJES y cada Dominio de cada peaje, tiene como Servidor NTP, el Gateway de su Red, siendo estos Gateway los Firewalls Corporativos (FORTIGATE). Estos obtienen la hora desde los Servidores de FORTIGUARD (Servicio conocido como "seguro" ya que FortiNet es una empresa que se dedica a Seguridad Corporativa).
Las fuentes utilizadas por Corporación Vial para tales efectos son los servidores de NTP de FortiNet: **ntp1.fortiguard.com, ntp2.fortiguard.com**

A.12.4.1 Registro de eventos.
PCI-DSS 10.6 Revisión de registros y eventos.

CVU tiene rutinas de controles diarios, donde se revisan las alertas de seguridad de los equipos FortiGate y OSSEC; también se realizan revisión en el sistema Graylog.
En caso de detectarse una anomalía o excepciones durante el proceso de revisión, se genera un ticket desde la herramienta Service Desk Manager y se deriva al responsable del equipo/área involucrada.

A.12.1.3 Gestión de capacidades.
PCI-DSS 10.6 Detección y notificación de fallas de sistemas críticos.

CVU cuenta con sistemas que permiten la detección y notificación en tiempo real sobre eventos de seguridad que puedan afectar la seguridad de la compañía.

A.12.4.3 Registros del administrador y el operador.

CVU ha desarrollado 2 procedimientos que se realizan de manera semestral.
Ellos son el Control de la Tabla Audito, donde se chequean semestralmente TODAS las operaciones "sensibles" o que pueden provocar "errores" dentro del sistema. En este control se observa, se valida y se verifica, que las personas que realizaron las operaciones "sensibles", cuenten con el perfil apropiado de acuerdo a su posición. Este procedimiento verifica desde los perfiles más básicos hasta los Administradores. Para evitar conflicto de intereses, este procedimiento lo realizan personas de áreas diferentes. Personal del CCO, por conocimiento de las actividades, y personal de Control de Gestión, como contraparte de auditoría.
El segundo es la Revisión periódica de usuarios, donde para el mismo período se consulta, controla y verifica que las personas que realizan actividades en el sistema, continúen trabajando y con el perfil apropiado. En caso de que ya no sea así, se actualiza la tabla de usuarios, cargando la "Fecha de Egreso".
Este procedimiento verifica desde los perfiles más básicos hasta los Administradores.

Documento Vinculado	Ruta de acceso al Documento
IN-TI-704 – CONTROL DE LA TABLA AUDITO V1.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-704
IN-TI-705 – REVISION PERIODICA DE USUARIOS V1.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-705

A.14.1 Política de control de acceso.
PCI-DSS 11 Probar regularmente los sistemas y procesos de seguridad.

CVU realiza escaneos de vulnerabilidades internos y externos de forma mensual, y/o en caso de cambios significativos en la red utilizando el Software Nessus Scan y/o OpenVAS. De detectarse hallazgos se corrigen conforme a los tiempos previstos por la norma.

CVU cuenta con 2 IP's Públicas (CVU y FACTE) contra Internet.
Asimismo, se exponen Servicios Web a usuarios a través de 3 Servidores adicionales.
Se debe realizar un control, para los siguientes puntos:

a) IP Pública Corporación Vial.
b) IP Pública Facturación Electrónica.
c) SRV-TESTING.
d) SRV-WSS
e) SRV-TCPTOLL

Toda esta información será registrada en el Registro RE-TI-721 –Escaneos de Vulnerabilidades con NESSUS "Año Corriente"
En caso de Detectar parches, los mismos deben ser instalados y registrados para cumplir el punto 6.2

Documento Vinculado	Ruta de acceso al Documento
RE-TI-721 – Escaneo de Vulnerabilidades con Nessus "Año Corriente"	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTRO APROBADOS\TI\RE-TI-721

Además, se realizan escaneos de vulnerabilidades ASV (Approved Scanning Vendor) externos de forma trimestral, y/o en caso de cambios significativos en la red. De detectarse hallazgos se corrección conforme a los tiempos previstos por la norma.

Se deberán registrar y tratar los hallazgos en el Sistema de Incidentes de Corporación Vial, con la misma categorización de hallazgos que indique el software utilizado.

Todo el tráfico dentro del alcance PCI, tiene aplicado perfiles de seguridad y se analizan mediante perfiles IPS (control y prevención de intrusos) configuración en los firewall de borde y de núcleo. Se han implementado sistemas que controlan la integridad de los archivos, mediante el sistema OSSEC. Cualquier modificación detectada es alertada por correo electrónico a la casilla del OSI, quién luego asigna vía ticket o notifica mediante llamada al encargado correspondiente.

A.13.1.1 Controles de red.
A.13.1.2 Seguridad de los servicios de red.
A.13.1.3 Separación de redes.
PCI-DSS 1.1.4 Firewall en cada conexión a Internet y entre cualquier red interna
PCI-DSS 1.1.5 Grupos, funciones y responsabilidades para administrar componentes de la red
PCI-DSS 1.1.6 Reglas de firewall y justificación de negocio
PCI-DSS 1.1.7 Revisión de las reglas de firewalls.

CVU ha invertido en los últimos años en mejorar y agregar seguridad a su red. Tanto a Nivel de Peajes, como a nivel de la Oficina Central.

En CVU la seguridad comienza por 2 pares de FIREWALLS CORPORATIVOS.
Cuenta con un cluster HA Fortigate de borde y un cluster HA Fortigate interno, lo que no permite conexiones a internet desde ningún punto de CVU sin la protección de un firewall, DMZ no existe.

FIREWALLS DE BORDE: Los de Borde son 2 FORTGATE 100G que trabajan en HA y por allí entran todos los servicios expuestos.
Los mismos controlan tráfico de Internet, tráfico en la Red de Peajes, tráfico de Globalmedia (Facturación Electrónica) y el tráfico de Teletrabajo o trabajo remoto de proveedores externos y del personal de CVU durante los períodos de trabajo.
Toda conexión a Internet y entre cualquier red interna, debe realizarse únicamente a través de estos equipos de seguridad, según los lineamientos de seguridad de CVU.
Al estar trabajando en ALTA DISPONIBILIDAD, cualquiera de ellos que FALLE, reportará la FALLA pero seguirá trabajando con el segundo dispositivo.
FIREWALLS INTERNOS: Para el control de tráfico Interno, contamos con otro par de FIREWALLS en HA que son 2 FORTIGATE 100E a través de los cuáles pasa todo el tráfico de la red interna.
Con estos ÍTEMS, cumplimos lo que pide la norma PCI-DSS como seguridad de tráfico.
Por debajo de estos FIREWALLS existen 2 Switches principales para los Servidores de Oficina Central y los Servidores de la red de PEAJES.
Estos son ARUBA 2540 que son Switches de **CORE/DISTRIBUCION** con Management.
CVU además cuenta con respaldo físico de ambos switches en su Stock.
Para **DISTRIBUCIÓN y ACCESO** usamos 6 Switches HP 1920S también con Management, donde se conectan los equipos de oficina, tanto del tramo OFICINA CENTRAL, como el tramo PEAJES.
Toda esta red está segregada por un esquema de vLANS de la siguiente manera:

vLAN 100 - vLAN de Management. Esta vLAN es usada para el cluster de Firewalls Internos, los vCENTER de las virtualizaciones, los Switches de Core, y los Switches de acceso.
vLAN 10 - vLAN de Servidores del tramo CVUNET. En esta vLAN solo se encuentran servidores del tramo 0, que ofrecen los Servicios a la Red de la Oficina Central.
vLAN 11 - vLAN de Servidores de Peajes. En esta vLAN solo se encuentran los servidores del tramo 1, que ofrecen servicios a la Red de Peajes.
vLAN 101 - vLAN de USUARIOS de Oficina Central. En esta vLAN solo se encuentran equipos de escritorio, notebooks y usuarios que usan servicios de los Servidores de la vLAN10.
vLAN 102 - vLAN de USUARIOS del Sistema de Peajes. En esta vLAN solo se encuentran equipos de escritorio, Notebooks y usuarios que usan servicios de los Servidores de la vLAN 11.
vLAN 103 - vLAN de Telefonía. En esta vLAN solo se encuentran los equipos y terminales de Telefonía IP de Corporación Vial.
vLAN 105 - vLAN de Seguridad. En esta vLAN se encuentran los Servidores que están ofreciendo servicios de seguridad: SIEM, OSSEC, CONSOLA ESET, WSUS, NAGIOS XI, ETC.
vLAN 107 - vLAN dedicada para Equipo de Manejo de Tarjetas de Crédito Aislado.
vLAN 108 - vLAN dedicada para Servidor de Notificaciones a Clientes (SMS, MAILS) con el fin de poder monitorear y controlar todo el tráfico que pasa ya que se comunica con el Servidor de BD, Telefonía e Internet.
vLAN 109 - vLAN dedicada a los Servicios de Facturación Electrónica.

Además de todo esto, CVU tiene licenciado el SOFTWARE NAGIOS XI.
Con este Software, se controlan todos los Servidores, Equipos, Servidores de Peaje, PC´s de Lectura de Matrículas, de todo el Sistema de Recaudación.

La administración de cualquier componente de la red (switches, firewalls, routers, etc) debe ser realizada por personal debidamente autorizado en los documentos RE-TI-705

Documento Vinculado	Ruta de acceso al Documento
RE-TI-705- Juan Curbelo.xlsx **RE-TI-705- Marcelo Martigani.xlsx** **RE-TI-705- Guillermo Pini.xlsx**	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\RE-TI-705 ARCHIVOS\CORPORACION VIAL\

Las reglas de firewall y su justificación se revisan cada tres meses.

Documento Vinculado	Ruta de acceso al Documento
Listado_Reglas_Justificadas.xlsx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\REGLAS DE FIREWALL\

A.13.2.2 Acuerdos sobre transferencia de información.
A.13.2.4 Acuerdos de confidencialidad o no divulgación.
A.14.1.3 Protección de las transacciones de servicios de aplicación.
Todas las transacciones generadas en el Sistema de Percepción de Recaudación de Peajes y a nivel de SAP, trabajan en sus respectivas bases de datos relacionales a nivel transaccional. Es decir que las mismas SOLO terminan ante el comando COMMIT, siendo revertidas, todas aquellas que no hayan llegado por cualquier motivo al final de la transacción, advirtiendo al usuario la NO CONCRESIÓN de las mismas. TRANSACT SQL.

A.15.1.1 Política de Seguridad de la Información para las relaciones con el proveedor.
A.15.1.2 Abordar la Seguridad dentro de los acuerdos del proveedor.
PCI-DSS 12.8
CVU ha agregado a sus contratos con proveedores externos de servicios, cláusulas de confidencialidad.
Asimismo, los permisos otorgados para los accesos VPN, son otorgados de manera limitada a las acciones y los servicios que deben acceder para el cumplimiento de sus funciones, no entregando ningún tipo de información o accesos, para aquellos recursos que no sean necesarios.

Este punto se cumple con la siguiente planilla

Documento Vinculado	Ruta de acceso al Documento
RI-TI-705-NombrEmpresa\RE-TI-705-nombreEmpleado.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\RI-TI-705-NombrEmpresa\RE-TI-705-nombreEmpleado.docx

A.15.1.3 Cadena de suministro de tecnologías de la información y comunicaciones.
A.15.2.1 Supervisión y revisión de los servicios del proveedor.

PCI-DSS 12.8.3
PCI-DSS 12.8.4
PCI-DSS 12.8.5

CVU realiza, previo al compromiso con un nuevo proveedor, una revisión de los riesgos de seguridad de los candidatos, a los efectos de asegurarse que los mismos cumplen con los requerimientos de seguridad que CVU establece y necesita.
Para los proveedores actuales, se realiza de forma anual una revisión y/o auditoría en caso de que corresponda, del cumplimiento de los aspectos de seguridad de la información que CVU requiere.

Cada Servicio suministrado por Proveedores Externos, es verificado por personal de CVU, al momento de terminar la tarea, o en su defecto en el siguiente ciclo de ejecución del Servicio.
De no obtener el resultado esperado, se envía notificación al proveedor para revisar los elementos afectados.

Este punto se cumple con la siguiente planilla

Documento Vinculado	Ruta de acceso al Documento
Evaluación de seguridad de Proveedores V1.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Evaluación de seguridad de Proveedores.docx

Documento Vinculado	Ruta de acceso al Documento
IN-GR-700 Guia y Condiciones de Uso de Telepeaje V10.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-GR-700

A.15 Relación con proveedores
PCI-DSS 12.9

CVU mantiene acuerdos y condiciones para el uso de los servicios de Telepeaje con todos los usuarios, donde se especifican que los datos del titular de la tarjeta al igual que cualquier otro dato personal, son protegidos conforme a lo establecido en la Ley de Protección de Datos Personales (Ley 18331).

A.6.1.3 CONTACTO CON LAS AUTORIDADES.
A.6.1.4 CONTACTO CON GRUPOS ESPECIALES DE INTERÉS.
PCI-DSS 12.10

CVU tiene un completo procedimiento para gestionar los incidentes de seguridad.
Este punto se cumple con la siguiente planilla

Documento Vinculado	Ruta de acceso al Documento
PR-TI-700 GESTION DE INCIDENTES.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\PR-TI-700

A.9.4 Control de acceso a sistemas y aplicaciones
PCI-DSS 2.2 ESTÁNDARES DE CONFIGURACIÓN Y HARDENING.
PCI-DSS 2.5 MANEJO DE CUENTAS POR DEFECTO.

Corporación Vial aplica un proceso de endurecimiento en las configuraciones los dispositivos Switches/Routers/Firewalls/Host Virtuales/Sistemas Operativos Windows. Se utiliza un checklist de configuraciones estándar según buenas prácticas y documentación de los fabricantes.

Es un procedimiento de checklist de configuración que se encuentra en el archivo "Estándares de Configuración y Hardening", que acompaña estas políticas.
Este checklist debe ser revisado de manera anual.

Documento Vinculado	Ruta de acceso al Documento
IN-TI-711 – CONFIGURACIÓN Y HARDENING	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS APROBADOS\IN-TI-711
Existe un Documento para los equipos en el Scope PCI específico para cada uno de estos equipos. El nombre de cada archivo es: HARDENING – "Nombre del equipo"	M:\CCO\CCOS SENSIBLE\SEGURIDAD DE LA INFORMACION\HARDENING

Corporación vial no permite utilizar/configurar servidores para varias funciones, en caso de ser necesario, este deberá ser analizado y aprobado por el Oficial de Seguridad.

A.8.1 Responsabilidad sobre los activos
PCI-DSS 2.4 INVENTARIO DE SISTEMAS EQUIPOS ALCANZADOS POR PCI-DSS.
PCI-DSS 9.7.1
PCI-DSS 9.7.2

Corporación Vial utiliza 2 Sistemas para dar tratamiento a los datos de PCI-DSS (Titulares y Tarjetas).
SRV-BD - Servidor virtualizado en Granja del dominio PEAJES. Este dominio NO TIENE contacto con Internet, y los datos de las tarjetas se encuentran grabados en un Microsoft SQL Server encriptadas por el Sistema de Recaudación.
El Acceso a la BD del Sistema de recaudación, está limitado a las personas que utilizan los datos para las altas, bajas y modificaciones. Ellos son los Operadores del CCO que tienen permiso de edición sobre estos datos, el Personal de TELSIS que desarrolla y mantiene el Sistema de Recaudación, y el Personal del Datacenter del CCO que son el personal jerárquico de Sistemas de Corporación Vial del Uruguay.
Jefe del Centro de Consolidación de Operaciones.
Analista de Hardware.
Analista de Software.
Todos los accesos tienen doble factor de autenticación.

Se realiza un control estricto de todo el inventario al menos una vez al año, o cuando se realicen cambios de relevancia que puedan afectar al mismo.

Este punto se cumple con las siguientes planillas

Documento Vinculado	Ruta de acceso al Documento
Inventario CVU.xlsx	M:\CCO\CCO SENCIBLE\SEGURIDAD DE LA INFORMACION**INVENTARIO TECNOLOGICO 2021\Inventario CVU**

A.8.2.3 Manipulado de la información
PCI-DSS 12.3.10 Prohibición de copiar, mover, almacenar datos de tarjetas.

CVU no permite copiar, mover o almacenar datos de tarjetas de crédito fuera del ambiente controlado existente.

A.13.1 Gestión de la seguridad de las redes

PCI-DSS 1.1 Establezca e implemente normas de configuración para firewalls y routers

En este punto de la norma, se detallan todos los controles con los que cuenta CVU a nivel de Firewall corporativo. No se incluyen aspectos de control y configuración en routers ya que el firewall auspicia como dicho rol en la red.

PCI-DSS 1.1.1.a Revise los procedimientos documentados para corroborar que existe un proceso formal para aprobar y probar lo siguiente:

- Conexiones de red
- Cambios en las configuraciones de firewalls y routers

CVU cuenta con un procedimiento que tiene como finalidad, realizar los cambios al Firewall Corporativo de manera segura, con solicitudes de cambios que sean aprobados por el Personal de TI de Corporación Vial del Uruguay, y llevados a cabo por la Empresa que brinda el Servicio de Mantenimiento a nuestra Red Corporativa o el OSI.
Cada jefe de Área solicitará los cambios necesarios a la configuración cerrada por defecto.

1. Si se detecta una necesidad de acceso a servicios, sistemas, o cualquier parte de la Red que no esté dentro de las funciones del perfil, el jefe del área deberá solicitar estos cambios a través del formulario de solicitud de nueva regla.

Este formulario cuenta con 2 secciones.
La Sección 1(AZUL) es para llenar cuando el cambio sea para una persona específica, y no para un grupo de personas.
La Sección 2(VERDE) es para llenar cuando el cambio afecte a un cargo o a un grupo de personas.

1) En Ambos casos se deberá completar si se trata de un ALTA, una BAJA, o una MODIFICACION a una regla existente.
2) Se debe individualizar a las personas afectadas por los cambios.
3) El Depto. de TI de CVU completará las direcciones IP en caso de ser necesarias, y los puertos a abrir en caso de ser necesarios.
4) El jefe solicitante debe completar claramente, cuáles son los nuevos sitios, servicios, accesos, o sistemas que se verán afectados.
5) El Depto. de TI de CVU completará el Origen y el Destino de la Regla.
6) Una vez aprobada por el personal del Depto. de TI de CVU, la misma será enviada a la empresa responsable de realizar estas actividades.
7) Los cambios serán probados por el Depto. de TI, verificando su correcta implementación, y dejando registro de la planilla de la Solicitud como Comprobante.
8) Una vez verificados todos los puntos el archivo quedará en el Repositorio para tales efectos.

Siguiendo el mismo lineamiento, en caso de requerirse un cambio en la configuración de los firewalls, como ser, por ejemplo, la actualización de firmware o registros internos, CVU cuenta con un formulario de cambios configuración firewall en donde se deja especificado:

1. Tipo de cambio a realizar
2. Estado original del cambio

3. Estado final del cambio
4. Definición de modificación
5. Descripción de tareas realizadas

Todos los cambios realizados, son aprobados antes, durante y luego de finalizado por el Jefe de Operaciones y TI.

Documento Vinculado	Ruta de acceso al Documento
IN-TI-710 – CAMBIOS A LOS FIREWALL CORPORATIVOS.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\INSTRUCTIVOS APROBADOS\IN-TI-710
RE-TI-724 – SOLICITUD DE NUEVA REGLA FIREWALL.docx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\RE-TI-724
RE-TI-726 – CAMBIO CONFIGURACION FIREWALL.xlsx	M:\SISTEMAS DE GESTION\DOCUMENTOS SGI\GESTION INTEGRADA\REGISTROS APROBADOS\RE-TI-726

A.13.1 – Gestión de la seguridad de las redes
PCI-DSS 1.1.2 Diagrama de red actual que identifica todas las conexiones entre el entorno de datos de titulares de tarjetas y otras redes, incluso cualquier red inalámbrica. El mismo debe incluir los flujos de datos de titulares de tarjetas entre los sistemas y las redes

CVU cuenta con un mapa de red corporativo en donde se especifican los servidores, dispositivos de red y canales de comunicaciones dentro del alcance PCI. En el mismo se detalla no solo la arquitectura de red, sino que también el flujo de datos de tarjetas de crédito dentro de dicho alcance.

No se incluyen redes inalámbricas ya que no se cuenta con dicha tecnología dentro de CVU.

A.13.1 Gestión de la seguridad de las redes
PCI-DSS 1.1.5 Descripción de grupos, funciones y responsabilidades para la administración de los componentes de la red.
PCI-DSS 1.1.6.a Verifique que las normas de configuración de firewalls y routers incluyan una lista documentada de todos los servicios, protocolos y puertos, incluida la justificación comercial y la aprobación para cada una.
PCI-DSS 1.1.7 Requisito de la revisión de las normas de firewalls y routers, al menos, cada seis meses.

De manera semestral, las políticas del Firewall deben de ser revisadas, de manera que, si se encuentra una regla obsoleta/vieja/que ya no aplica, la misma debe ser removida. Se deberá dejar registro en la planilla de control de Reglas del Firewall, la fecha en que se realiza, quien lo realiza, y si encontró elementos obsoletos para remover.

A.13.1 Gestión de la seguridad de las redes
PCI-DSS 1.2.1 Restrinja el tráfico entrante y saliente a la cantidad necesaria para el entorno de datos de los titulares de tarjetas y niegue específicamente el tráfico restante.
PCI-DSS 1.2.2 Asegure y sincronice los archivos de configuración de routers

CVU mantiene un Contrato de Mantenimiento con la Empresa AT Sistemas, y cuenta con 4 Firewalls, 2 de Borde trabajando en HA y 2 Perimetrales trabajando en HA. Las únicas personas autorizadas para acceder a los Firewall corporativos son:
Personal de Servicio de AT Sistemas.
Jefe del Centro de Consolidación de Operaciones.
Analista de Hardware.
Analista de Software.
Todos los Firewalls trabajan en HA y su configuración está sincronizada de manera continua por esta condición. Además, se realizan 2 Backup semanales por parte del OSI.

A.12.2 Protección contra el software malicioso
PCI-DSS 1.4 Instale software de firewall personal o una funcionalidad equivalente en todos los dispositivos móviles.
Firewall de Windows habilitado en todos los equipos por GPO, el usuario no puede deshabilitarlo
Se debe tener en cuenta el firewall de cada dispositivo móviles (notebooks en teletrabajo) y en los puestos de trabajo que acceden a datos de tarjetas de crédito

A.12.1 Procedimientos y responsabilidades operacionales
A.13.1 Gestión de la seguridad de las redes
PCI-DSS 1.5 Asegúrese de que las políticas de seguridad y los procedimientos operativos para administrar los firewalls estén documentados, implementados y que sean de conocimiento para todas las partes afectadas.

La administración de los firewalls utilizados por CVU se realiza siguiendo la documentación oficial de los fabricantes, acorde a las versiones vigentes de los mismos.

Documento Vinculado	Ruta de acceso al Documento
FortiOS-7.2.3-Administration_Guide.pdf	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI

A.11 Seguridad física y del entorno
PCI-DSS 7 Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa
PCI-DSS 7.1 Limite el acceso a los componentes del sistema y a los datos del titular de la tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso.
PCI-DSS 8.1 Identificar y autenticar el acceso a los componentes del sistema.
PCI-DSS 9.10 Asegúrese de que las políticas de seguridad y los procedimientos operativos para restringir el acceso físico a los datos del titular de la tarjeta estén documentados, en uso y sean conocidos por todas las partes afectadas.

Corporación Vial del Uruguay cuenta con restricciones de acceso para la administración de todos los dispositivos o sistemas de la empresa. Todos los usuarios son nominados para los accesos a sistemas donde se almacenan datos de tarjeta de crédito y dispositivos administrables (switches, routers, etc)

Se toma como punto de partida la asignación de mínimos privilegios necesarios y se otorga accesos privilegiados únicamente a los roles requeridos según la clasificación y función de su trabajo.

En cuanto a la administración de dispositivos de red, servidores y aplicaciones únicamente el grupo DATACENTER tiene privilegios totales para realizar cambios y configuraciones. El mismo es integrado por los 3 administradores que tiene CVU los cuales tiene como rol principal asegurar la disponibilidad de todos los sistemas críticos de la empresa.

El acceso a los sistemas donde se ingresan/guardan/almacenan/procesan datos de tarjetas de crédito está controlado por el firewall de la red y únicamente los usuarios Operadores del CCO tienen permisos controlados.
Para acceder al PC encargado del ingreso y/o procesamiento de datos de tarjeta, se debe realizar mediante escritorio remoto desde ubicaciones específicas de la oficina y con usuarios habilitados para tal tarea. No se permite ingresar ni sacar documentos y/o información desde este dispositivo.

Asimismo, el acceso a este equipo está protegido por un 2FA (DUO) que permite acceso únicamente a los usuarios que tengan la herramienta configurada.

A continuación, se describen los permisos de cada sistema o aplicación y se justifica la necesidad de cada rol que deba tener permisos de administrador a un sistema o acceso de escritura y lectura sobre datos de tarjetas de crédito:

TCP-TOLL
Dicho software se utiliza para la administración del sistema global de recaudación.

Únicamente los Administradores de CVU y Asistentes de Mesa de Ayuda tienen permisos de escritura y lectura sobre datos de tarjetas de crédito. El resto de los usuarios, tienen específicamente deshabilitado dicho permiso.

TCP-PP
Dicho software se utiliza para procesar los archivos de tarjetas de crédito y realizar el envío de las mismas a las contrapartes correspondientes.

GES
Dicho software se utiliza para:

- Administración de TAGS
- Notificaciones a los usuarios (mail y SMS)
- Altas de archivos de tarjetas de crédito
- Gestión de la plataforma web y app de telepeajes

Dentro de dicho software únicamente los administradores de CVU y los Asistentes de Mesa de Ayuda tiene permisos para utilizar la funcionalidad de "importar y procesar altas masivas de tarjetas de crédito". El único lugar en donde el usuario puede visualizar el número de la tarjeta de crédito es en la funcionalidad de "Importar". Igualmente, debe tener permisos para ingresar a dicha funcionalidad para que esto sea posible.

Este punto se cumple con la siguiente planilla

Documento Vinculado	Ruta de acceso al Documento
RE-TI-706 – GESTIÓN DE RIESGOS POR ACTIVOS	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI

A.11.2 Seguridad de los equipos
PCI-DSS 12.3 Desarrolle políticas de uso para las tecnologías criticas y defina como usarlas correctamente.
PCI-DSS 12.3.1 Aprobación explícita de las partes autorizadas.
PCI-DSS 12.3.2 Autenticación para el uso de la tecnología.
Cada vez que un funcionario entienda pertinente instalar cualquier clase de software, que no esté comprendido en listado de software aprobado por la organización, en algún equipo propiedad de CVU deberá solicitar la aprobación al oficial de seguridad de la información.
Solo los usuarios administradores tienen permisos de instalación de software.

- **Proceso**

El requerimiento de instalación deberá ser acompañado por un Formulario de Solicitud de Software.xlsx
dónde se especifique el motivo de dicha necesidad, el cual deberá estar "firmado" por el responsable del área.
En base al mismo el OSI evaluará las implicancias de seguridad que ello pudiera tener y aprobará o no dicha solicitud.
Este punto se cumple con la siguiente planilla

Documento Vinculado	Ruta de acceso al Documento
Lineamientos Generales Uso de Tecnologías V2.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Lineamientos Generales Uso de Teconologias_V2.docx
RE-TI-728 Formulario de Solicitud de Software.xlsx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\RE-TI-728 – FORMULARIO DE SOLICITUD SOFTWARE.xlsx

PCI-DSS 12.3.3 Listado de dispositivos y personal con acceso

A.11.2 Seguridad de los equipos
PCI-DSS 12.3.6 Ubicaciones de red aceptables para las tecnologías
Las ubicaciones aceptadas para el equipamiento se detallan a continuación por tipo de dispositivo:

PC - Notebook: se ubicará en el escritorio correctamente y conectado a la boca de red que se requiera según las tareas que desempeñe (CVUNET-PEAJES)

Servidores: Se ubicará en el centro de datos debidamente rackeados y conectados al switch de core, con las vlan que corresponda asignadas según el fin de los mismos.

Storages: Se ubicará en el centro de datos, debidamente rackeados y conectados por hilos de fibra

a los servidores que corresponda según el fin de los mismos.

Firewalls: Se ubicará en el centro de datos, debidamente rackeados.
Switches administrables: se ubicará en el centro de datos, debidamente rackeados.

Switches tontos: se ubicarán de ser necesarios (con previa evaluación) para la multiplicación de puertos, en las cercanías de los puestos de trabajo que lo requieran.

A.7.2 Seguridad relativa a los Recursos Humanos.
PCI-DSS 12.6 Programa de sensibilización.
PCI-DSS 12.7 RRHH
CVU cuenta con un programa de sensibilización de anual.

Documento Vinculado	Ruta de acceso al Documento
PG-TI-701 Cronograma de Concientización CVU 2023.xlsx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Cronograma de Concientización CVU.xlsx

CVU cuenta con procesos bien definidos para la búsqueda, incorporación, permanencia (durante el lapso de vinculación) y salida del personal, según los siguientes documentos.

Documento Vinculado	Ruta de acceso al Documento
Política de RRHH.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Política de RRHH.docx
Procedimiento ante ingresos y egresos de Recursos Humanos.docx	M:\CCO\CCO SENSIBLE\SEGURIDAD DE LA INFORMACION\PESI\Procedimiento ante ingresos y egresos de Recursos Humanos.docx

Montevideo, 1° de noviembre de 2023

Sr. Ángel Fachinetti — Director

Ec. José Luis Puig — Presidente