Contenido

1. OBJETIVO 2
2. ALCANCE 2
3. DEFINICIONES 2
4. CIFRADO EN LA TRANSMISION DE DATOS EN RTVC 5
5. FIRMAS DIGITALES 7
6. FIRMAS ELECTRÓNICAS 7

VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1	DIANA ROJAS LUIS MERLY TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	LAURA MARCELA PERDOMO FONSECA	20/11/2020	Versión inicial
2	JAKELINE SÁNCHEZ MERLY AMPARO TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	17/05/2022	Actualización

1. OBJETIVO

Propender porque la información de mayor nivel de sensibilidad de RTVC, se encuentre cifrada durante su transmisión.

2. ALCANCE

Este documento está dirigido principalmente a usuarios administradores de red, firewall y servidores, para que sea aplicado en todas las plataformas y aplicaciones de RTVC que procesen información o datos clasificados como sensibles, confidenciales u otra que requiera protección criptográfica.

3. DEFINICIONES:

Algoritmo de cifrado: Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico.[1]

Cifrado: Es un método de codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.[2]

Criptoanálisis: Es la ciencia que se ocupa de estudiar herramientas y técnicas que permitan romper los códigos y sistemas de protección definidos por la criptografía.[3]

Criptografía: Es la ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar (encriptar o cifrar) la información. Mediante la criptografía es posible garantizar la confidencialidad, integridad, disponibilidad y la autenticidad de los mensajes y documentos guardados en un sistema o red informática.[4]

1 Glosario de Términos de ciberseguridad - INCIBE
2 Tomado de la ISO/IEC 27000:2013
3 Enciclopedia de la Seguridad Informática. 2ª edición - Álvaro Gómez Vieites - Pág. 361
4 Enciclopedia de la Seguridad Informática. 2ª edición - Álvaro Gómez Vieites - Pág. 361

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.[5]

No repudio: El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.[6]

Firma digital o electrónica: Métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permiten identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente. [7] La firma electrónica es un género que incluye la firma digital.

Integridad: La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.[8]

Certificado digital: Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet. El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación.[9]

Cifrado simétrico: también conocido como cifrado de clave secreta, es la técnica más antigua y en ella se utiliza la misma clave para cifrar y descifrar la información.[10]

Cifrado asimétrico: es una técnica de codificación que utiliza un par de claves diferentes para el cifrado y descifrado de información. Los sistemas de criptografía asimétrica se basan en la generación de un par de claves, denominadas clave pública

5 Tomado de la ISO/IEC 27000:2013
6 Glosario de Términos de ciberseguridad - INCIBE
7 Decreto 2364 de 2012
8 Glosario de Términos de ciberseguridad - INCIBE
9 Glosario de Términos de ciberseguridad - INCIBE
10 Glosario de Términos de ciberseguridad - INCIBE

y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra.[11]

Llaves Criptográficas: Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

SEGURIDAD DE LA CAPA DE TRANSPORTE (TLS): es un protocolo que proporciona cifrado y seguridad para los datos enviados entre un cliente y un servidor. El protocolo Transport Layer Security (TLS) añade una capa de seguridad sobre los protocolos de transporte TCP/IP. TLS usa cifrado simétrico y cifrado de llave pública para enviar datos privados de forma segura, y añade características de seguridad adicionales, como autenticación y detección de manipulación de mensajes

Red privada virtual (VPN): Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

11 Glosario de Términos de ciberseguridad - INCIBE

4. CIFRADO EN LA TRANSMISION DE DATOS EN RTVC

Se debe hacer uso de protocolos seguros de comunicación para garantizar la confidencialidad al acceder a los sistemas de la entidad, tanto si los colaboradores se encuentran dentro de la entidad o fuera de ella. Entre otros se incluyen los siguientes protocolos:

- SSH para el acceso seguro remoto a la administración de equipos (no utilizar Telnet debido a que la comunicación va en texto plano, no cifrado)
- SFTP/FTPS para la transferencia segura de archivos
- HTTPS para la transferencia segura de datos en servicios web de la entidad

WEB

- Se utilizarán mecanismos criptográficos para el establecimiento de canales seguros de comunicación vía Web, a través de protocolos seguros como HTTPS y SFTP, en todos los sitios Web de la entidad.

- Las comunicaciones entre las dependencias de RTVC y las entidades bancarias con las que se realizan transacciones, deben hacerse a través de canales seguros de comunicación.

CORREO ELECTRÓNICO

- RTVC utiliza mecanismos de transferencia segura del correo electrónico a través de los certificados digitales dispuestos en la solución en Google, tanto para el SmartKey (inicio de sesión), como la de correo electrónico propiamente.

TRANSFERENCIA DE ARCHIVOS

- La transferencia de archivos debe realizarse a través de protocolos seguros como SFTP.

VPN

- RTVC dispone de mecanismos para la conexión segura con los sistemas y dispositivos al interior de la entidad.

- La Coordinación de T.I. proveerá el servicio de conexión remota a la plataforma tecnológica institucional a través de red privada virtual (VPN por sus siglas en inglés), con lo cual el tráfico de datos entre usuario remoto y red institucional se encontrará debidamente cifrado.
- Sólo usuarios previamente autorizados por la Coordinación de T.I. podrán utilizar el servicio VPN, los que, además, serán los responsables del correcto uso del servicio de acceso remoto.
- Cada usuario solo podrá tener activa una única conexión VPN con RTVC y debe desconectarla una vez concluida las operaciones a realizar en la red interna.
- Los usuarios del sistema VPN serán automáticamente desconectados de la sesión, una vez que hayan transcurrido máximo 1 hora de inactividad. Si el usuario es desconectado deberá iniciar sesión nuevamente para volver a conectarse a la red

ADMINISTRACIÓN REMOTA

- El ingreso para la gestión remota de dispositivos como equipos de comunicaciones, de seguridad o servidores, debe estar restringida, permitiendo solo usuarios conectados a través de la VPN.

- La gestión de los equipos de red o servidores a través interfaz de línea de comando (CLI) se debe realizar sin excepción a través del protocolo SSH V2 (Secure Shell) que garantice que las contraseñas se envíen cifradas.

- El ingreso para la gestión remota de Sistemas de información o aplicaciones debe estar restringida, permitiendo solo usuarios conectados a través de la VPN.

RED WIFI

- Se configurará la red WIFI de la entidad con el estándar de cifrado más seguro, actualmente WPA2, y cambiaremos su clave de acceso por defecto.

5. FIRMAS DIGITALES

- Se hará uso de la firma digital de conformidad con la circular de Gerencia “Trámite de firmas de la gerencia y documentación en general” y el manual “Manual de firma digital”.

- La Coordinación de T.I. se encargará del proceso de generación y entrega a los servidores públicos que así lo requieran, previa autorización del ordenador del gasto o Gerente de RTVC.

6. FIRMAS ELECTRÓNICAS

Se hará uso de las firmas electrónicas de conformidad con la circular 010 de 2021 y el manual “Firmas electrónicas para contratistas y proveedores”.