CONTENIDO

Índice de Tablas

VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1.0	DIANA ROJAS LUIS MERLY TORRES BERNAL	LAURA MARCELA PERDOMO FONSECA	LAURA MARCELA PERDOMO FONSECA	2020-29-10	Versión inicial

1 INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación realiza la selección de controles, y durante la fase de Implementación ejecuta la implementación de controles de seguridad de la información en RTVC, basados en la norma ISO 27001:2013 y su Anexo A de controles, con los lineamientos y buenas prácticas de la norma ISO 27002:2013.

La información es un recurso que, como el resto de los activos, tiene valor para RTVC y por consiguiente debe ser debidamente protegida. Las políticas operacionales de seguridad y privacidad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, reducir los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la entidad.

RTVC, como entidad pública cumpliendo con la normativa y estándares vigentes que dictan las entidades del Gobierno Nacional según su competencia, en el presente lineamiento compila los controles implementados para cada uno de los dominios del Anexo A de controles de la norma.

2 OBJETIVO

Proponer los mecanismos y herramientas para la aplicación de los controles de Seguridad de la Información y Seguridad Digital, con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información dentro de RTVC, de acuerdo al ciclo PHVA, (planear, hacer, verificar y actuar), con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

3 ALCANCE

Este documento aplica a todas las dependencias de RTVC, funcionarios, colaboradores, terceros, a sus recursos y procesos, con el fin de establecer, implementar, mantener y controlar el Sistema de Gestión de Seguridad de la Información de RTVC.

4 TABLA DE CONTROLES

La tabla 1 muestra la organización de los controles, su aplicación y evidencias, detallando los 14 dominios y 114 objetivos de control de acuerdo con el Anexo A de la norma ISO 27001.

Tabla 1 – Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

No	DOMINIO - CONTROL		APLICA (SI/NO)	EVIDENCIA
A.5	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**			
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**			
0bjetivo. Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.				
A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	SI	Se cuenta con políticas de seguridad de la información por cada uno de los dominios. I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4. Políticas de Seguridad de la Información y Seguridad Digital
A.5.1.2	Revisión de las políticas para la seguridad de la información.	Control. Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	Se realiza la revisión y aprobación por parte del Comité Institucional de Gestión y Desempeño; en casos especiales por cambios en la Organización, o en la operación estos serán revisados de manera oportuna.

.

A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**			
A.6.1	**Organización interna**			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.				
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Se cuenta con la I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital, donde se discriminan los roles en seguridad de la información. Las cuales se encuentran en Kawak 4.6.1.1 Roles y Responsabilidades
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	SI	Se cuenta con la Resolución 147 de 2018, donde se crea el Comité Institucional de Gestión y Desempeño de Radio Televisión Nacional de Colombia- RTVC. Se cuenta la Política Operacional de Seguridad de la Información y Seguridad Digital, donde se discriminan los roles en seguridad de la información. Las cuales se encuentran en Kawak.

.

A.6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	SI	Se cuenta con el Documento Contacto con autoridades y grupos de interés especial.
A.6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad	SI	Se cuenta con el Documento Contacto con autoridades y grupos de interés especial. Se tiene contacto con el Ministerio de las TIC y con CSIRT Gobierno
A.6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak

A.6.2	**Dispositivos móviles y teletrabajo**			
Objetivo: Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles				
A.6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	I-A-3 Política Operacional para la administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.7.2. Administración de la Red Inalámbrica 4.9.7. Acceso a WLAN
A.6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	SI	Boletín No. 50 del 26 de marzo de 2020, el cual señala que, como parte del compromiso con la transformación digital, RTVC – Sistema de Medios Públicos, mediante la Resolución 473 de 2017, adoptó el teletrabajo en modalidad suplementario, como una forma de organización laboral a distancia, utilizando como soporte las tecnologías de la información y las comunicaciones. H-F-20 Solicitud Incorporación del Teletrabajo

A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes de asumir el empleo**			
Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.				
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	SI	Procedimiento H-P-5 Procedimiento Selección y Contratación de Personal Formato H-F-14 Formato de Requisición de personal Revisión Antecedentes: Procuraduría, Contraloría, Policía y extranjeros (Interpol)
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	Procedimiento H-P-5 Procedimiento Selección y Contratación de Personal Formato H-F-14 Formato de Requisición de personal Revisión Antecedentes: Procuraduría, Contraloría, Policía y extranjeros (Interpol)

A.7.2	**Durante la ejecución del empleo**			
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.				
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratista la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.4. Lineamientos para la Gestión de la Seguridad de la Información y de las Seguridad Digital Contrato de Trabajo.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la in formación.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	H-P-4 Proceso de Desarrollo y formación de Personal y Evaluación de Desempeño
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	B- P -1 Control Disciplinario B-A-1 Política Operacional de Control de Asuntos Disciplinarios
A.7.3	**Terminación y cambio de empleo**			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	H- P-3 Proceso de Desvinculación I- F-14 Formato de Certificado de Paz y Salvo Informático H -F- 13 Formato de Entrevista Retiro de Trabajo Formato P-F-21 Formato de aprobación para la terminación Anticipada S-M-2 Manual Administrativo y Financiero para el manejo de contratos de Administración Delegada
A.8	**GESTION DE ACTIVOS**			
A.8.1	**Responsabilidad por los activos**			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.				
A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	Se cuenta con la Matriz de Inventario y Clasificación de activos de la Información Se cuenta con la Guía para la Gestión y clasificación de activos de Información

A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	SI	Se cuenta con la Matriz de Inventario y Clasificación de activos de la Información Se cuenta con la Guía para la Gestión y clasificación de activos de Información
A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.4. Lineamientos para la Gestión de la Seguridad de la Información y de las Seguridad Digital
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	I-F-14 Formato Certificado Paz y Salvo Informático I- A-2 Política Operacional para la Administración de la Infraestructura de TI

A.8.2	**Clasificación de la información**			
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.				
A.8.2.1	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Se cuenta con el documento de Gestión y Clasificación de Activos de Información y la Matriz de Inventario y Clasificación de Activos de Información
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se cuenta con el documento de Gestión y Clasificación de Activos de Información Se cuenta con la Matriz de Inventario y Clasificación de Activos de Información Se cuenta con el Procedimiento de Etiquetado de Información
A.8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se cuenta con el documento de Gestión y Clasificación de Activos de Información Se cuenta con la Matriz de Inventario y Clasificación de Activos de Información Se cuenta con el Procedimiento de Etiquetado de Información

A.8.3	**Manejo de medios**			
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios				
A.8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2. Seguridad del equipo fuera de RTVC 4.9.3. Escritorio y Pantalla limpia

A.8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI R-A-2 Política operacional de Gestión Ambiental R-S-1 Plan Institucional de Gestión Ambiental RTVC 5.3 Condición Ambiental Institucional
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Criptografía

A.9	**CONTROL DE ACCESO**			
A.9.1	Requisitos del negocio para el control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.				
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI
A.9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI
A.9.2	Gestión de acceso de usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.				
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	Si	Política Operacional de Seguridad de la Información y Seguridad Digita Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos

A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	Si	Política Operacional de Seguridad de la Información y Seguridad Digita Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.5 Acceso a los dispositivos
A.9.3	Responsabilidades de los usuarios			
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.				
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak

A.9.4	Control de acceso a sistemas y aplicaciones			
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.				
A.9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO

A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO

A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak b. CONTROL DE ACCESO LÓGICO
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	Si	El Líder Soluciones de Software - Desarrollo es quien autoriza el manejo y control del código fuente. T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC 6. Políticas de Desarrollo de Software
A.10	**CRIPTOGRAFIA**			
A.10.1	Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información				
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.7. CRIPTOGRAFÍA Se cuenta con el documento de Criptografía
A.10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	Si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.7. CRIPTOGRAFÍA Se cuenta con el documento de Criptografía

A.11	**SEGURIDAD FISICA Y DEL ENTORNO**			
A.11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A.11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico

A.11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.5	Trabajo en áreas seguras.	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.6.3. POLÍTICAS DE CONTROL DE ACCESO a. Control de Acceso Físico
A.11.1.6	Áreas de carga, despacho y acceso público	Control: Se deben controlar los puntos de acceso tales como las áreas de despacho y carga y otros puntos por donde pueden entrar personas no autorizadas y, si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI	Las áreas de cargue y despacho se encuentran aisladas de las áreas de procesamiento de información
A.11.2	Equipos			
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.				
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9 Políticas de Usuarios 4.9.1 Equipos de computo
A.11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas Generales
A.11.2.3	Seguridad en el cableado.	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas Generales
A.11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2 Políticas de Mantenimiento Preventivo de la Infraestructura Tecnológica

A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2 Seguridad de equipos fuera de RTVC.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.9.2 Seguridad de los equipos fuera de RVC
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak 4.9.3 Escritorio y pantalla limpia
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.9.3 Escritorio y pantalla limpia
A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.				
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	I - P-7 Proceso Gestión de Incidentes Internos I- P- 9 Proceso Mantenimiento Preventivo Tecnológico Interno I-P-10 Proceso Monitoreo Tecnológico Interno T-P-1 Proceso Planificación de la Infraestructura Tecnológica T-P-4 Proceso Soluciones de Software T-S-1 Plan de Continuidad del Negocio
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Pendiente el proceso Gestión de Cambios
A.12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Pendiente el proceso Gestión de la Capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores

A.12.2	Protección contra códigos maliciosos			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.				
A.12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con la consola de Antivirus BitDefender, por medio de él se tiene control de tráfico de todo lo que pase por la Red.
A.12.3	Copias de respaldo			
Objetivo: Proteger contra la perdida de datos				
A.12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI 4.2.2 Políticas de Backup
A.12.4	Registro y seguimiento			
Objetivo: Registrar eventos y generar evidencia				
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores Las herramientas no permiten borrar los logs, si se desea realizar alguna actividad esta debe ser exportada para poder trabajar los logs de las actividades.
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	I- A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak 4.3.2 Servidores Todo registro que se realice independiente del rol desempeñado queda registrado en los logs de los sistemas
A.12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	Los relojes se sincronizan con Hora Legal Colombiana del INM

A.12.5	Control de software operacional			
Objetivo: Asegurarse de la integridad de los sistemas operacionales				
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.12.6	Gestión de la vulnerabilidad técnica			
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas				
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	Se realiza anualmente el Análisis de Vulnerabilidades y Ethical Hacking.
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak
A.12.7	Consideraciones sobre auditorias de sistemas de información			
Objetivo: Minimizar el impacto de las actividades de auditoria sobre los sistemas operativos				
A.12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	Se cuenta con Logs de Auditorías y las auditorías a los sistemas de información se encuentran debidamente programadas, las cuales quedan registradas en el formato
A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	Gestión de la seguridad de las redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.				
A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red
A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red

A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak Se cuenta con Firewall Perimetral Se cuenta con el Diagrama de Red
A.13.2	Transferencia de información			
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.				
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.		I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak
A.13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital I -A-2 Política Operacional para la Administración de la Infraestructura de TI Las cuales se encuentran en Kawak "Cualquier copia, uso o distribución no autorizados de este mensaje y sus adjuntos puede generar responsabilidades legales. • Si usted no es destinatario de este correo, por favor notifíquelo al remitente. • Aplicamos la Ley Estatutaria 1581 de 2012, que protege el derecho de acceso a la información pública. • Antes de imprimir este mensaje, compruebe si es necesario hacerlo. El Medio Ambiente es cuestión de TODOS."
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	Se cuenta con acuerdos de confidencialidad con funcionarios, proveedores y clientes debidamente firmados. Contrato laboral.
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1	**Requisitos de seguridad de los sistemas de información**			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.				
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak Se realiza Sensibilización y Capacitación en Seguridad de la Información.

A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-F-1 Formato requerimientos iniciales para el desarrollo Web y Aplicaciones Las cuales se encuentran en Kawak
A.14.2	Seguridad en los procesos de Desarrollo y de Soporte			
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.				
A.14.2.1	Política de desarrollo seguro	Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software T-F-1 Formato requerimientos iniciales para el desarrollo Web y Aplicaciones Las cuales se encuentran en Kawak
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	si	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.5	Principio de Construcción de los Sistemas Seguros.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak
A.14.3	Datos de prueba			
Objetivo: Asegurar la protección de los datos usados para pruebas.				
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC T-P-4 Proceso Soluciones de Software Las cuales se encuentran en Kawak

A.15	**RELACIONES CON LOS PROVEEDORES**			
A.15.1	Seguridad de la información en las relaciones con los proveedores.			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.				
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak. Se cuenta con los acuerdos contractuales, Pólizas y Seguros.

A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital T-A-3 Política Operacional de Desarrollo e Implementación de Software para RTVC Las cuales se encuentran en Kawak Acuerdos de confidencialidad firmados con los proveedores
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI	Se tienen en los contratos firmados con los proveedores que los mismos se comprometen a hacer cumplir las políticas de seguridad de la información Acuerdos de confidencialidad firmados con los proveedores
A.15.2	Gestión de la prestación de servicios de proveedores			
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores				
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	Se realizan auditorías a los proveedores de tecnología de la información y las comunicaciones.
A.15.2.2	Gestión del cambio en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	SI	Se tienen establecidas cláusulas en los contratos firmados con los proveedores.

A.16	**GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**			
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.				
A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Procedimiento de Gestión de Incidentes En los perfiles se tiene establecido que todos los funcionarios deben reportar los diferentes incidentes que se puedan presentar en la organización.
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	Procedimiento de Gestión de Incidentes

A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI	Procedimiento de Gestión de Incidentes

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	SI	Procedimiento de Gestión de Incidentes
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Procedimiento de Gestión de Incidentes
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	SI	Procedimiento de Gestión de Incidentes
A.16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	Procedimiento de Gestión de Incidentes
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTION DE CONTINUIDAD DE NEGOCIO**			
A.17.1	Continuidad de Seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI	T-S-1 Plan de Continuidad del Negocio
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	T-S-1 Plan de Continuidad del Negocio Falta la Implementación
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	T-S-1 Plan de Continuidad del Negocio Falta las pruebas
A.17.2	Redundancias			
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.				
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Control: Las instalaciones de procesamientos de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	T-S-1 Plan de Continuidad del Negocio Se cuenta con redundancia en equipos y no de instalaciones. Diagrama de Red

A.18	**CUMPLIMIENTO**			
A.18.1	Cumplimiento de requisitos legales y contractuales			
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.				
A.18.1.1	Identificación de la legislación aplicable.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	SI	Se cuenta con la Matriz de Verificación de Requisitos Legales de Seguridad de la información. La Organización cumple con los lineamientos y normatividad exigida por el Ministerio de las TIC.
A.18.1.2	Derechos propiedad intelectual (DPI)	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	Se cuenta con la Matriz de Verificación de Requisitos Legales de Seguridad de la información. La Organización cumple con los lineamientos y normatividad exigida por el Ministerio de las TIC.
A.18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	Cuenta con las tablas de retención documental de acuerdo con las disposiciones del Archivo General de la Nación.
A.18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	Se cuenta con el documento J-A-3 Política Operacional de Protección de Datos
A.18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Documento Criptografía Se cuenta con los Procedimientos de Controles Criptográficos
A.18.2	Revisiones de seguridad de la información			
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.				
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información), se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI	Se realizan auditorías, revisión de políticas y procedimientos.

A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI	I-A-3 Política Operacional de Seguridad de la Información y Seguridad Digital Las cuales se encuentran en Kawak Se cuenta con la Matriz de Verificación de Legalidad
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Anualmente se realizan pruebas de Vulnerabilidades Técnicas.

5 BIBLIOGRAFÍA

- ISO/IEC 27001:2013, NORMA TÉCNICA NTC-ISO. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) REQUERIMIENTOS.
- ISO/IEC 27002:2005, NORMA TÉCNICA NTC-ISO. TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.
- Guía No. 8 Controles de Seguridad y Privacidad Ministerio de las Tic.