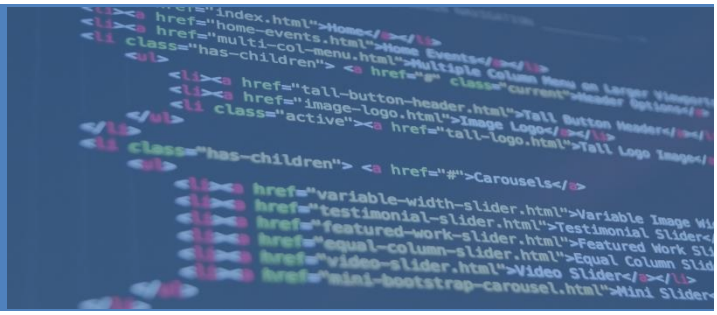


OFERTA SISTESEG:
CISO AS A SERVICE

Tabla de Contenido

Control de Versiones:

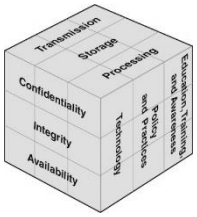
Versión	Capítulo	Fecha	Descripción
1.0	Todos	15/08/2024	Elaboración del documento
2.0	Todos	30/08/2024	Actualización del documento

Control de Aprobaciones:

Versión	Preparado Por	Verificado Por	Aprobado por
1.0			
2.0			

INTRODUCCIÓN

Por medio del presente documento se presenta la oferta que tiene como objetivo principal exponer las actividades para realizar en el plan de trabajo **CISO AS A SERVICES** que cumpla con lograr los objetivos de preservar **la Confidencialidad, la Integridad y la Disponibilidad (CIA) de la información** durante **su Transmisión, Almacenamiento o Transmisión (TAT)** y considerando aspectos como **la Autenticación, Autorización y Registro de eventos (AAR) y las Personas, Procesos y Tecnologías (PPT).** Estos doce aspectos son fundamentales cuando se trata de mejorar la seguridad de la información en un mundo no exento de riesgos impulsados por nuevas tecnologías como la inteligencia artificial, deep and machine learning, natural language process y LLM (large language model and transformers).



DESCRIPCIÓN DEL DOCUMENTO

El documento Plan de Trabajo **CISO AS A SERVICE** incluye las actividades que se realizarán con relación a la protección de los activos de información apoyado en la norma **ISO 27001-27002:2022-2013,** la norma **PCI DSS 4.0.1** y **la ley 1581 del 2012** durante el periodo definido para la prestación de este servicio. Es importante recalcar que este plan de trabajo toma como entradas la realización de un diagnóstico en los dominios de las normas mencionadas y, otras normas, que se tengan consideradas en la estrategia corporativa de tecnologías de información.

NORMAS CONSIDERADAS PARA LA PRESTACIÓN DEL SERVICIO

En la siguiente tabla se exponen los dominios de la norma que se tendrán como guía durante la ejecución del servicio. La norma ISO 27001:2022-2013 y la norma PCI DSS v 4.0.1, estas cubren tanto aspectos tecnológicos como aspectos administrativos. Se considerará en una etapa inicial los dominios que por sus características poseen una injerencia directa en los controles tecnológicos que se deben implementar.

Una vez concluida esta labor procederemos a abordar los dominios que se denominan administrativos. En las siguientes tablas se presentan los dominios que conforman las normas:

Dominio ISO 27001	Objetivo de control
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Ilustración 1. Dominios del GAP según ISO 27001.

REQUERIMIENTOS PCI DSS 4.0.1
1. Instalar y mantener una configuración de los controles de seguridad de red para proteger la información sensible.
2. Utilizar estándares de configuración segura para los componentes del alcance.
3. Proteger los datos almacenados sensibles.
4. Cifrar la transmisión de los datos de los datos sensibles a través de redes públicas abiertas.
5. Usar y actualizar con regularidad la protección contra malware.
6. Desarrollar y mantener sistemas y aplicaciones seguras.
7. Limitar el acceso a los datos de los titulares, únicamente a lo que los negocios necesiten saber.
8. Asignar una identificación única a cada persona con acceso a una computadora.
9. Restringir el acceso físico a los datos de los titulares de tarjetas.
10. Rastrear y monitorear todo acceso a los recursos de la red y a los datos sensibles.
11. Probar con regularidad los sistemas y procesos de seguridad.
12. Mantener una política que aborde la seguridad de la información.

Ilustración 2. Dominios del GAP según PCI DSS.

DIAGNÓSTICO

La realización de un diagnóstico con respecto al nivel de madurez de la norma ISO 27001:2013-22022 es un componente fundamental del desarrollo de la prestación del servicio **CISO AS A SERVICE.** Para la realización de esta actividad se requiere realizar entrevistas con los administradores de los diferentes componentes de la infraestructura. En estas entrevistas se recolectará información relacionada con la gestión desde el punto de vista de seguridad por parte del administrador. También, se inspeccionarán estos dispositivos con el fin de verificar que exista una configuración segura y su respectiva documentación.

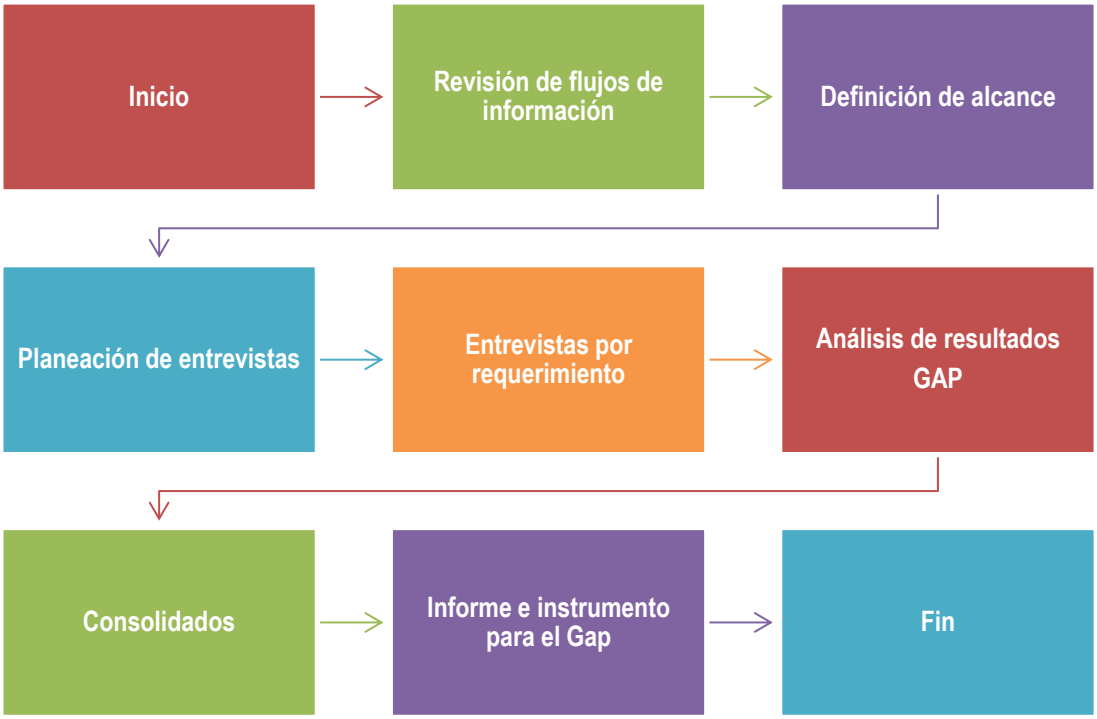


Ilustración 3. Fases del diagnóstico

A continuación, haremos una descripción detallada de los pasos con que cuenta nuestra metodología de análisis de GAP con relación a la norma ISO 27001:2013-2022, la cual consideramos el punto central de la definición de una estrategia de la arquitectura de seguridad de la información, perfectamente alineada con la visión de la organización, dentro de su entorno de operación. El Gap Análisis (análisis de brecha) considera los diferentes dominios de ISO 27001 con el fin de evaluar la distancia a la que la organización se encuentra de cumplirla en un 100%. La seguridad de la información es como tal un proceso de mejora continua, y no necesariamente un llegar a este valor del 100%, ya que esta es una decisión que compete a la organización, teniendo en cuenta presupuestos, amenazas y riesgos en general. A continuación, un ejemplo del resultado obtenido por medio del Gap.

Para la ejecución del diagnóstico de situación actual de seguridad de la información en **el cliente** se realizarán entrevistas, inspecciones en sitio y revisiones documentales sobre las áreas de cumplimiento

de la norma ISO 27001:2013-2022 con el fin de verificar el cumplimiento de los requisitos de seguridad. Los resultados se consolidarán en tablas de cumplimiento. Para cada área evaluada se generará adicionalmente un análisis y una recomendación preliminar. Los resultados globales se consolidaron en un resumen ejecutivo y los resultados particulares en tablas de evaluación por requisito. Finalmente se generarán conclusiones del análisis de brecha.

NUMERAL	CLAUSULA	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
A.5	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	30%	70%	100%	Repetible
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	13%	87%	100%	Inicial
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	73%	27%	100%	Administrado
A.8	GESTIÓN DE ACTIVOS	13%	87%	100%	Inicial
A.9	CONTROL DE ACCESO	34%	66%	100%	Repetible
A.10	CRIPTOGRAFÍA	20%	80%	100%	Inicial
A.11	SEGURIDAD FÍSICA	38%	62%	100%	Repetible
A.12	GESTIÓN DE OPERACIONES	23%	77%	100%	Repetible
A.13	SEGURIDAD DE LAS COMUNICACIONES	20%	80%	100%	Inicial
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	19%	81%	100%	Inicial
A.15	RELACIONES CON LOS PROVEEDORES	15%	85%	100%	Inicial
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	14%	86%	100%	Inicial
A.17	CONTINUIDAD DE SEGURIDAD DE LA INFORMACION	5%	95%	100%	Inicial
A.18	CUMPLIMIENTO	21%	79%	100%	Repetible
PROMEDIO CLAUSULAS		24%			Repetible

Ilustración 4. Dominios del análisis de brecha.

Con el propósito de determinar la conformidad del cliente con los objetivos de control y los controles de seguridad propuestos en el anexo A de la norma NTC ISO/IEC 27001 se llevarán a cabo las siguientes actividades con el propósito de lograr los objetivos propuestos:

Evaluar cuantitativa y objetivamente el estado de los controles de seguridad que se consideran aplicables para determinada organización

1. Determinar los controles aplicables al tipo de organización tomando como referente una buena práctica internacional (ISO/IEC 27001:2013-2022, PCI DSS 4.0.1).

2. Determinar los controles necesarios según la legislación aplicable a la organización.

3. Determinar mediante entrevistas con preguntas cerradas de dos opciones si los controles aplicables son implementados satisfactoriamente.

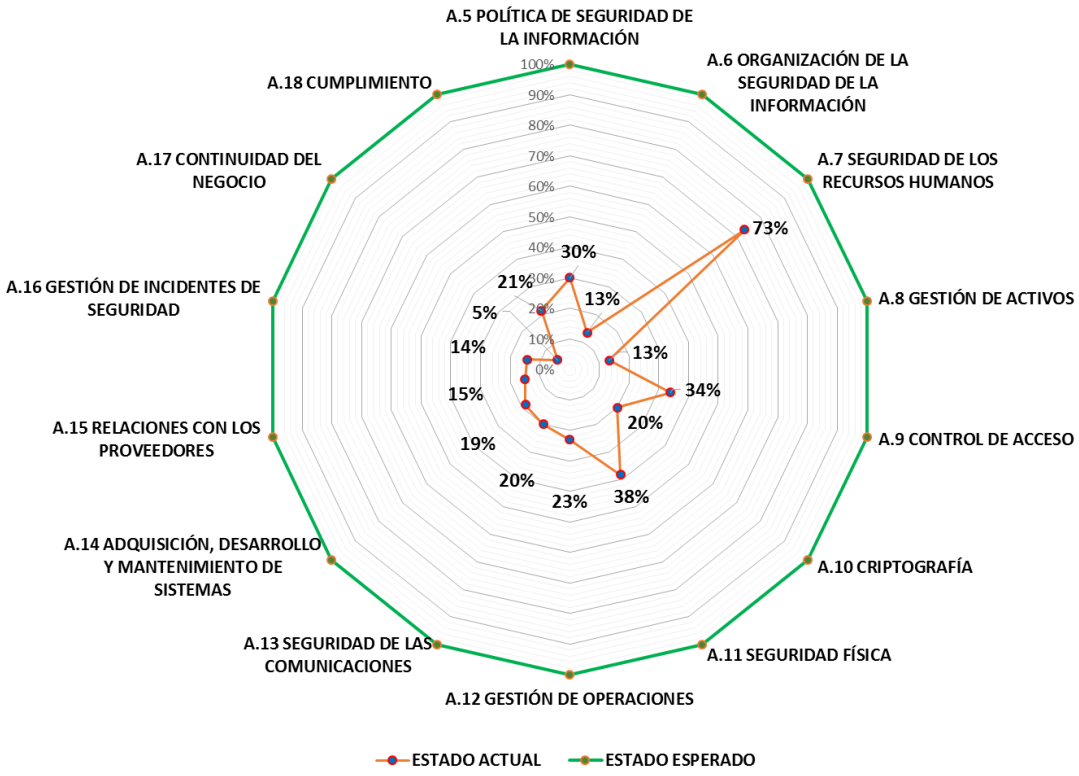


Ilustración 5. Presentación de los resultados del GAP**.**

Se busca cubrir con este estudio, en el análisis de controles, todas las áreas de control especificadas en las buenas prácticas internacionales. Analizar los controles relacionados con políticas de seguridad de la información, organización de la seguridad de la información, gestión de los activos, seguridad de los recursos humanos, seguridad física y del entorno, entrega de Servicios de TI y de telecomunicaciones, control de acceso, adquisición, el desarrollo y el mantenimiento de los sistemas de información, gestión de los incidentes de seguridad, gestión de continuidad del negocio y cumplimiento.

Se busca presentar los resultados cuantitativos por control y área de control y los aspectos relevantes de mejora para cada dominio de control:

1. Para cada control de cada dominio de control se determinará el porcentaje de cumplimiento respecto de los aspectos aplicables.

2. Para cada dominio de control se determinará el porcentaje de cumplimiento a partir del estado de los controles que lo conforman.

3. Presentar sugerencias relevantes que conduzcan a incrementar la efectividad del control en la organización.

A continuación, presentamos las tareas a realizar para obtener resultados cuantitativos por control y área de control y los aspectos relevantes de mejora para cada dominio de control:

GENERALIDADES DEL PLAN DE TRABAJO

La estructura, desde un alto nivel de las actividades que desarrollará el CISO se pueden enmarcar en un análisis de contexto de la organización con el fin de que las actividades realizadas estén alineadas tanto con la estrategia de tecnologías de la información como con las estrategias de alto nivel estratégicas.

Es fundamental para el desarrollo de las actividades del CISO que antes de iniciar cualquier plan de remediación de implementación de algún control de seguridad, se realice un diagnóstico de cumplimiento. Con base en los resultados de este diagnóstico de definirá el PESI o plan estratégico de seguridad de la información. Una vez elaborado el anterior documento se procede a mantener un ciclo de seguimiento, complementado con una labor de revisión continua hasta que se logre el cumplimiento propuesto en el plan de acción.

En el siguiente diagrama se puede observar lo descrito anteriormente:

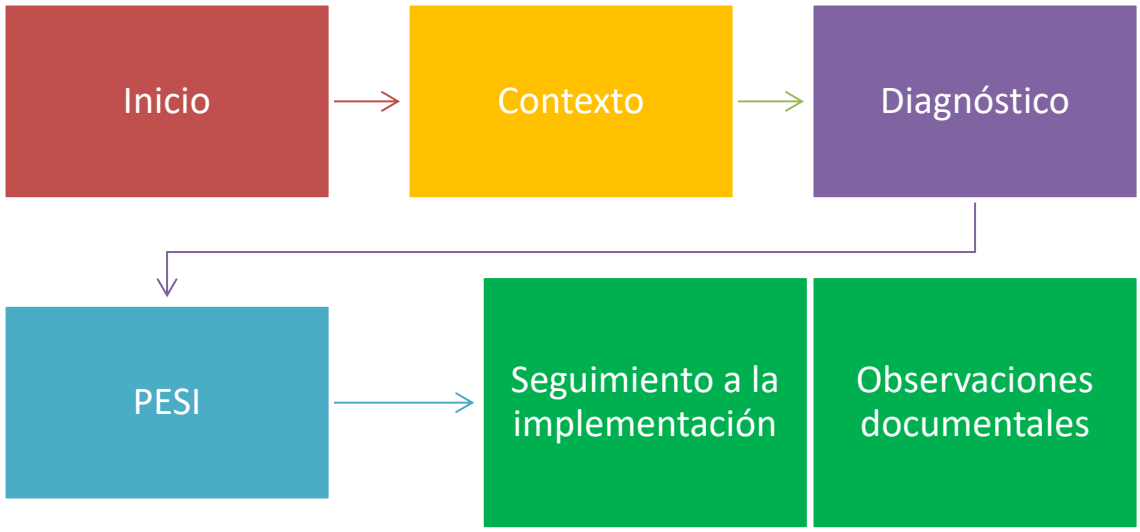
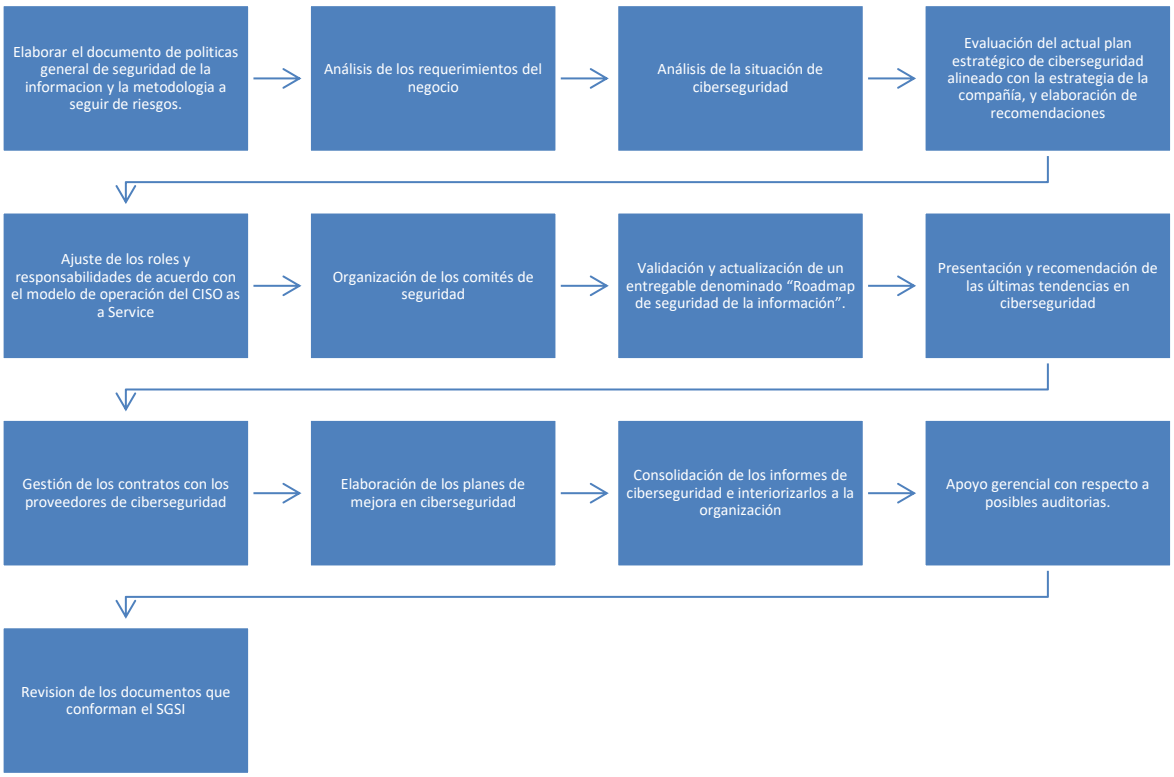


Ilustración 6. Metodología del servicio CISO**.**

En el contexto se busca comprender los objetivos misionales y el PESI existente. El diagnóstico es fundamental para entender el nivel de madurez en ciberseguridad y este termina en la actualización de este PESI. Así se continua con el seguimiento a la implementación el cual se controla por medio de las preauditorias y las calificaciones obtenidas de las auditorías externas o internas, según el caso. Estas dos últimas fases se continúan realizando hasta el fin del servicio.

PLAN DE TRABAJO DETALLADO

Las actividades que hacen parte de Plan de Trabajo parten del análisis de los requerimientos del negocio. En el siguiente diagrama se puede observar las actividades del producto: **CISO AS A SERVICE**.



CRONOGRAMA 2024-2025

DOMINIOS TECNOLÓGICOS

A continuación, presentamos de manera detalladas los dominios de tecnológicos de la norma ISO 27001:2013 los cuales serán aquellos abordados en la primera fase del proceso del diagnóstico. También se aclara las respectivas responsabilidades del CISO en cada uno de estos dominios.

Control de acceso: En este dominio el CISO tendrá como principal responsabilidad gestionar los accesos a todos los componentes de la infraestructura con el objetivo de preservar la confidencialidad, la integridad y la disponibilidad de la información.

CONTROL DE ACCESO	A.9
Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	**A.9.1**
Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**A.9.1.1**
Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	**A.9.1.2**
Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	**A.9.2**
Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	**A.9.2.1**
Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	**A.9.2.2**
Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**A.9.2.3**
La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	**A.9.2.4**
Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	**A.9.2.5**
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.	**A.9.2.6**
Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	**A.9.3**
Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	**A.9.3.1**
Se debe evitar el acceso no autorizado a sistemas y aplicaciones.	**A.9.4**
El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.	**A.9.4.1**
Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	**A.9.4.2**

Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	**A.9.4.3**
Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	**A.9.4.4**
Se debe restringir el acceso a los códigos fuente de los programas.	**A.9.4.5**

Criptografía: En este dominio el CISO debe velar porque la información sensible sea transmitida, recibida o almacenada de tal manera que se preserve su integridad y su confidencialidad.

CRIPTOGRAFÍA	A.10
Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles.	**A.10**
Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	**A.10.1**
Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	**A.10.1.1**
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.	**A.10.1.2**

Seguridad física y del entorno: Como parte de la seguridad de la información el CISO en este dominio debe procurar que la información sea protegida por amenazas que afecten su nivel de disponibilidad.

SEGURIDAD FÍSICA Y DEL ENTORNO	A.11
Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	**A.11.1**
Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.	**A.11.1.1**
Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	**A.11.1.2**
Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**A.11.1.3**
Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**A.11.1.4**
Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	**A.11.1.5**
Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**A.11.1.6**
Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	**A.11.2**
Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	**A.11.2.1**
Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	**A.11.2.2**

El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información deben estar protegido contra interceptación, interferencia o daño.	**A.11.2.3**
Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	**A.11.2.4**
Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	**A.11.2.5**
Se debe 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.	**A.11.2.6**
Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	**A.11.2.7**
Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	**A.11.2.8**
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.	**A.11.2.9**

Seguridad de las operaciones: El día a día dentro de una organización moderna se rige por una serie de actividades que de no realizarse de manera rigurosa se pudiese tener una afectación de la información.

SEGURIDAD DE LAS OPERACIONES	A.12
Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	**A.12.1**
Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	**A.12.1.1**
Se debe 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.	**A.12.1.2**
Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	**A.12.1.3**
Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**A.12.1.4**
Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	**A.12.2**
Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**A.12.2.1**
Proteger contra la pérdida de datos.	**A.12.3**
Se debe hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	**A.12.3.1**
Registrar eventos y generar evidencia.	**A.12.4**

Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**A.12.4.1**
Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**A.12.4.2**
Las actividades del administrador y del operador del sistema se debe registrar, y los registros se deben proteger y revisar con regularidad.	**A.12.4.3**
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.	**A.12.4.4**
Asegurar la integridad de los sistemas operacionales.	**A.12.5**
Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.	**A.12.5.1**
Prevenir el aprovechamiento de las vulnerabilidades técnicas.	**A.12.6**
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.	**A.12.6.1**
Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	**A.12.6.2**
Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.	**A.12.7**
Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	**A.12.7.1**

Seguridad de las comunicaciones: En este dominio el CISO debe velar porque la información sensible sea transmitida o recibida de tal manera que se preserve su integridad y su confidencialidad.

SEGURIDAD DE LAS COMUNICACIONES	A.13
Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	**A.13.1**
Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	**A.13.1.1**
Se debe 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	**A.13.1.2**
Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**A.13.1.3**
Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	**A.13.2**
Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	**A.13.2.1**
Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	**A.13.2.2**
Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	**A.13.2.3**

Se debe 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.	**A.13.2.4**

Gestión de incidentes: En este dominio el CISO debe velar porque la información sensible sea transmitida o recibida de tal manera que se preserve su integridad y su confidencialidad.

GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	A.16
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
Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	A.16.1.1
Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	A.16.1.2
Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	A.16.1.3
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.	A.16.1.4
Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	A.16.1.5
El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	A.16.1.6
La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	A.16.1.7

Adquisición, desarrollo y mantenimiento de sistemas: En este dominio el CISO debe velar porque la información sensible sea protegida durante todo el ciclo de desarrollo.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14
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 en redes públicas.	A.14.1
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.	A.14.1.1
La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	A.14.1.2
La información involucrada en las transacciones de los servicios de las aplicaciones se debe 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.	A.14.1.3

Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2
Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	A.14.2.1
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.	A.14.2.2
Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	A.14.2.3
Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	A.14.2.4
Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	A.14.2.5
Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	A.14.2.6
La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	A.14.2.7
Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.	A.14.2.8
Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.	A.14.2.9
Asegurar la protección de los datos usados para pruebas.	A.14.3
Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	A.14.3.1

BIBLIOGRAFÍA

- ISO/IEC 27001: 2013-2022. Sistemas de gestión de la seguridad de la información.
- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- NTC 5254 Gestión del riesgo.
- PCI DSS 4.0

ANEXO ESTÁNDARES DE SEGURIDAD

- ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, August 1999
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003
- NIST SP 800-55 Security Metrics Guide for Information Technology Systems, July 2003
- NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002
- NIST SP 800-45 Guidelines on Electronic Mail Security, September 2002
- NIST SP 800-44 Guidelines on Securing Public Web Servers, September 2002
- NIST SP 800-42 Guideline on Network Security Testing, October 2003
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy, January 2002
- NIST SP 800-40 Procedures for Handling Security Patches, September 2002
- NIST SP 800-36 Guide to Selecting Information Security Products, October 2003
- NIST SP 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000
- NIST SP 800-21 Guideline for Implementing Cryptography in the Federal Government, November 1999
- NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems, December 1998
- NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- NIST SP 800-13 Telecommunications Security Guidelines for Telecommunications Management Network, October 1995
- NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
- NIST SP 800-6 Automated Tools for Testing Computer System Vulnerability, December 1992
- NIST SP 800-5 A Guide to the Selection of Anti-Virus Tools and Techniques, December 1992
- PCI DSS 4.0V 3.1

GLOSARIO DE TÉRMINOS

Actividades críticas: Operaciones críticas y/o actividades que soportan los objetivos de la entidad.

Activo: Cualquier cosa que tenga valor para la organización.

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:

1. **Personas:** Incluyendo sus calificaciones, competencias y experiencia.
2. **Intangibles:** Ideas, conocimiento, conversaciones.
3. **Electrónicos:** Bases de datos, archivos, registros de auditoria, aplicaciones, herramientas de desarrollo y utilidades.
4. **Físicos:** Documentos impresos, manuscritos y hardware.
5. **Servicios:** Servicios computacionales y de comunicaciones.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo

Área IT: Es el área encargada de soportar, diseñar y mantener los activos electrónicos y el hardware propiedad de la entidad.

Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.

Consultor: Persona idónea en capacidad de prestar servicios de asesoría, diseño, y creación de propiedad intelectual.

Custodio: Encargado de proteger la información por delegación del propietario. Generalmente este rol es ejecutado por el Área IT.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Estándares: Un producto o mecanismo especifico el cual es seleccionado desde un punto de vista universal, para su uso a lo largo de toda la organización, con el objetivo fundamental de soportar una política ya aceptada y aprobada por las directivas de la entidad.

Información: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil...) de un conjunto de conocimientos. Por ejemplo:

1. Una noticia que escuchamos por la radio.
2. Una señal de tráfico que advierte un peligro.
3. Una fórmula que usamos en un problema.

La información se representa mediante conjuntos de símbolos, que pueden ser de diferente naturaleza:

1. Textuales o numéricos, como las letras y números que usamos al escribir.
2. Sonoros, como los fonemas, las notas musicales...

3. Cromáticos, como los colores de los semáforos.
4. Gestuales, como los que usamos para hacer mímica.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

PCI: Payment Card Industries

Procedimientos: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.

Propietario: Es el responsable y dueño del activo de información. Define también sus niveles de clasificación.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Tarjetahabiente: Persona que utiliza medios de pagos por medio de tarjetas de crédito.

Terceros: Entendemos por terceros a proveedores, contratistas, clientes y visitantes al Sistema.

Usuario: Es el que utiliza los activos de información para llevar a cabo las funciones de su trabajo.

	FORMATO DE CONTROL DE CAMBIO		**Contrato N.°:** **Cambio N.°:**
CLIENTE:			
PROYECTO:			
INFORMACIÓN			
Solicitado por:		Fecha:	
Descripción del cambio:			
APROBACIÓN PARA EL ANÁLISIS			
Por xxx: Sí / No:		Por (Cliente): Sí / No:	
Nombre y cargo:		Nombre y cargo:	
Fecha:		Fecha:	
ANÁLISIS			
Impacto general del cambio:			
Impacto en tiempo:	+/-	Impacto en RR. HH.	+/-
Impacto en precio:	+/- $	Con cargo a:	
Comentarios:			
Analizó en:		Analizó en (Cliente):	
Cargo:		Cargo:	
Fecha:		Fecha:	
APROBACIÓN			
Por xxx: Sí / No:		Por (Cliente): Sí / No:	
Nombre y cargo:		Nombre y cargo:	
Fecha:		Fecha:	
Observaciones:			