Contenido

1. INTRODUCCIÓN

Un Programa de Control Operacional para garantizar la seguridad de la información consiste en una serie de actividades programadas a lo largo del tiempo con el propósito de implementar, revisar y asegurar que los controles establecidos para la gestión de riesgos a los que la organización está expuesta sean ejecutados de acuerdo con lo definido.

La información se considera un recurso valioso para la organización, similar a otros activos, y, por lo tanto, debe ser protegida de manera adecuada. Las políticas de seguridad y privacidad de la información se encargan de resguardar contra diversas amenazas, asegurando así la continuidad de los sistemas de información, minimizando los riesgos de daño y garantizando el cumplimiento eficiente de los objetivos de las entidades gubernamentales.

Durante la fase de Planificación del modelo de seguridad y privacidad de la información, se lleva a cabo la selección de los controles de seguridad que se implementarán en la fase actual, esto también basado en la matriz de riesgos identificados.

La implementación de estos controles en relación con la seguridad de la información se ajusta al ciclo de mejora continúa conocido como PHVA (Planear, Hacer, Verificar y Actuar), siguiendo las directrices del Modelo de Seguridad y Privacidad de la Información (MSPI) desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

2. OBJETIVO

Presentar el plan de implementación de tratamiento de riesgos y controles de seguridad alineados con la política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información – MSPI.

3. GLOSARIO

- **ACTIVO DE INFORMACIÓN**: Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.
- **DIRECTORIO ACTIVO (Active Directory):** es un servicio que almacena información acerca de los objetos de una red (usuarios, equipos, grupos, políticas, etc.) facilitando su búsqueda y uso por parte de los usuarios y administradores.
- **DISPONIBILIDAD DE LA INFORMACIÒN:** En el campo de la seguridad de la información, la disponibilidad es la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de las personas autorizadas.
- **INTEGRIDAD DE LA INFORMACIÒN:** Es una propiedad de la información que 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.
- **PROCESO:** Secuencia de actividades que uno o varios sistemas desarrollan para hacer llegar una determinada salida (output) a un usuario, a partir de la utilización de determinados recursos (entradas/input).

- **CONFIDENCIALIDAD DE LA INFORMACIÒN:** Principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.
- **SEGURIDAD DE LA INFORMACIÓN:** Conjunto de medidas preventivas y reactivas que permiten garantizar la confidencialidad, integridad y disponibilidad de la información.
- **VULNERABILIDAD:** Debilidad existente en un sistema que puede ser utilizada por personas malintencionadas para comprometer su seguridad.

4. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la información y las Comunicaciones
NTC_ISO/IEC 27035:2011, tecnología de la información	Técnicas de seguridad – gestión de incidentes de seguridad de la información
NTC-ISOI/EC 27001- 27002:2013	normativa que permite asegurar y proteger la información física y digital.
Decreto 2693 de 2012 MinTic	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
LEY 1915 DE 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos
Decreto 1008 de 2018 MinTic	Se establecen los lineamientos generales de la política de Gobierno Digital.
Resolución 945 de 2018	Por medio de la cual se crea el Comité Institucional de Gestión y Desempeño del Departamento de Arauca.
Decreto 1414 de 2017 de MinTic.	Se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones-MINTIC
CONPES 3854 de 2016.	Política Nacional de Seguridad digital.
Ley 1712 de 2014	Se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
Decreto 1377 de 2013	Reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales

LEY 1712 DE 2014.	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1266 de 2008	Se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
REFERENTES DE POLÍTICA DIGITAL	
Manual de seguridad y privacidad de la información – MINTIC - Estrategia de Gobierno Digital.	
Controles de Seguridad y Privacidad de la Información, guía No. 8	

5. TABLA DE CONTROLES

La siguiente tabla muestra los controles de seguridad de la información en la estructura correspondiente al Anexo A de la norma NTC: ISO/IEC 27001.

El contenido de la tabla obedece a la siguiente estructura:

A.X – Dominio
A.X.X – Objetivo de Control
A.X.X.X - Controles

6. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad, es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información. Este proceso se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requeridas por la Entidad).

El siguiente es el formato de Declaración de aplicabilidad a aplicar como actividad posterior a la evaluación de riesgos:

		Objetivo de control o control seleccionado Si/No.	Razón de la Selección.	Objetivo de control o control Implementado Si/No.	Justificación de exclusión.	Referencia	Aprobado por la alta dirección Firma director de la entidad.
Dominio	**A.X**						
Objetivo del Control	A.X.X						
Control	A.X.X.X						
Control	A.X.X.X						

REVISÓ	APROBÓ
PROFESIONAL UNIVERSITARIO REQUERIMIENTOS TECNOLOGICOS	GERENTE

Revisó Aspectos de Calidad: Lorena Aguirre, Profesional Universitario - Planeación

CONTROL DE CAMBIOS			
FECHA	DESCRIPCION DEL CAMBIO	VERSION	MODIFICADO POR
10/04/2021	Aprobada por Comité de Institucional de Gestión y Desempeño	1	Profesional Universitario de Requerimientos Tecnológicos.
22-02/2022	Aprobada por Comité de Institucional de Gestión y Desempeño	2	Profesional Universitario de Requerimientos Tecnológicos.
30/01/2023	Actualización Aprobada por Comité de Requerimientos Tecnológicos.	3	Profesional Universitario de Requerimientos Tecnológicos.
28-12-2023 30/01/2024	Actualización Socializada y Viabilizada por Comité de Institucional de Gestión y Desempeño No 13. Actualización aprobada por Comité de Institucional de Gestión y Desempeño No 01.	4	Comité Institucional de Gestión y Desempeño