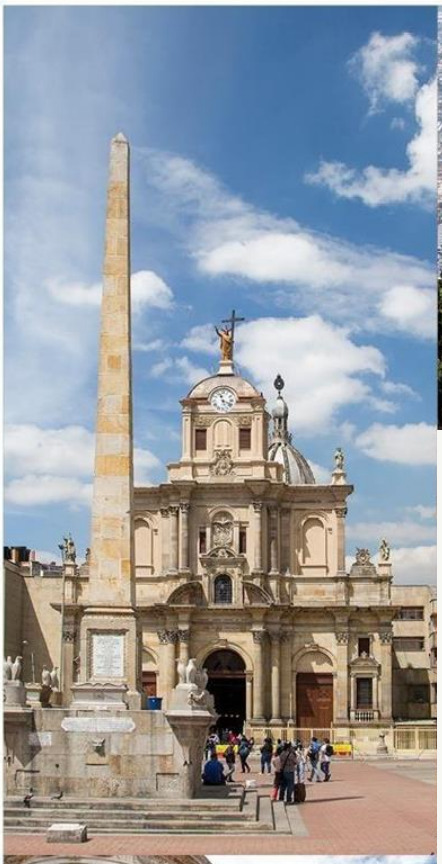
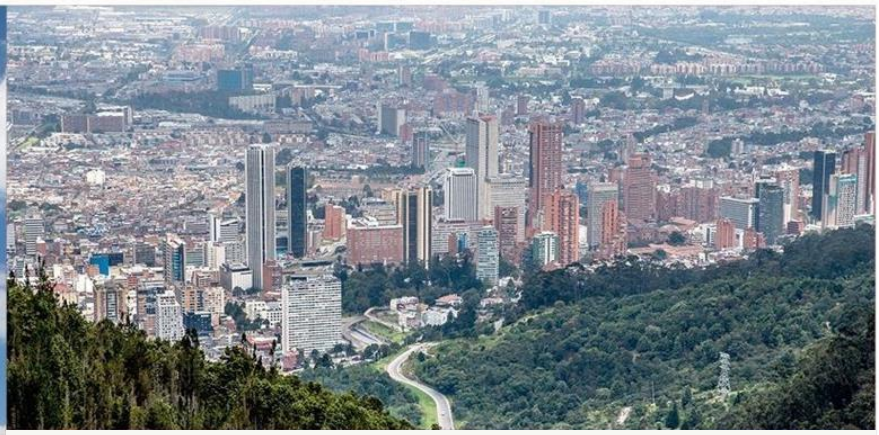
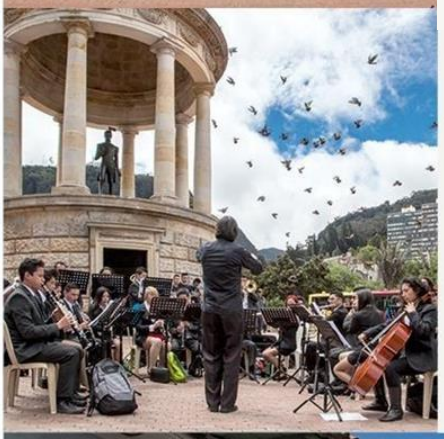




INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital del Patrimonio Cultural



Plan

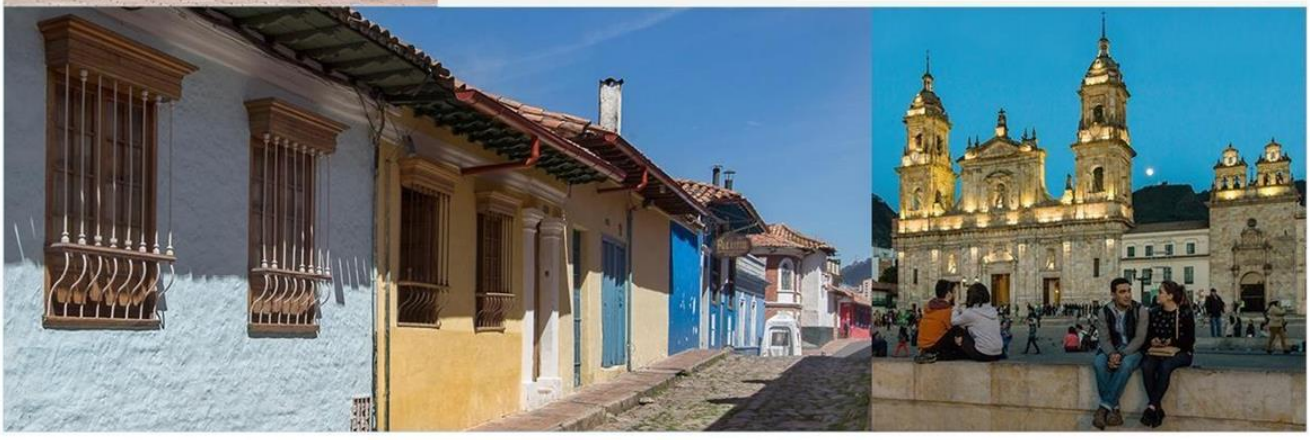
Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Proceso

Gestión de Sistemas de Información y Tecnología

Vigencia: 31 de enero 2022

Versión: 03



1. OBJETIVO

Fortalecer la gestión de riesgos de seguridad de la información mediante un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que apoye la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos de Seguridad Digital, preservando la Confidencialidad, Integridad y Disponibilidad de la información, acorde con los requerimientos de la entidad y en relación con el cumplimiento de requisitos legales y reglamentarios pertinentes a la legislación colombiana.

2. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aplica para todos los procesos de la entidad, incluyendo las actividades para la gestión del riesgo a través de la Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas y Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas, logrando así la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

3. DEFINICIONES

TÉRMINO	DEFINICIÓN
Amenaza	Ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Concientización	Acción que se relaciona con tomar conciencia de un asunto determinado, mostrarle una verdad a través del diálogo y hacerle reflexionar sobre un asunto concreto.
Control	Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Impacto	Consecuencias que genera un riesgo una vez se materialice.

Información	Datos organizados de tal forma que tienen un significado.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
Partes interesadas	Son todos aquellos individuos, grupos u organizaciones que tengan algún beneficio o perjuicio, relacionado con los intereses y actividades de la entidad.
Probabilidad	Posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo, en otras palabras, qué tan posible es que el riesgo se materialice.
Riesgo	Escenario de incertidumbre, bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitándole cumplir con sus objetivos.
Sensibilización	Proceso de comunicación activo que promueve transformación, cambio de actitudes y comportamientos en las personas de la entidad.
Tecnología de la Información	Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.
Vulnerabilidad	Falencia o debilidad que es inherente a los activos de información o a los controles.

4. NORMATIVIDAD

Ley 23 de 1982. Ley sobre derechos de autor.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

Ley Estatutaria 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.

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución Distrital 305 de 2008, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital.

Norma ISO 31000:2018.

5. ACTIVIDADES PLAN

La implementación para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

ID	ACTIVIDADES	RESPONSABLE	PRODUCTOS
1	Actualización metodología de riesgos de seguridad digital.	Oficial de Seguridad de la Información.	Metodología de riesgos de seguridad digital.
2	Sensibilización riesgos de seguridad digital.	Oficial de Seguridad de la Información.	Actas de reunión y/o correos electrónicos.
3	Identificación de Activos de Información. Clasificación de Activos de Información. Valoración de Activos de Información	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos valoración riesgos y/o correos electrónicos.
4	Identificación de Amenazas y Vulnerabilidades. Determinación del Impactos de las amenazas por activo Determinación de Probabilidad de Ocurrencia	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos valoración riesgos y/o correos electrónicos.
5	Identificación y valoración riesgos de seguridad digital.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos valoración riesgos y/o correos electrónicos.
6	Determinación de Controles Tratamiento de Riesgos Diseño de controles Priorización de	Procesos IDPC.	Formatos valoración riesgos y/o correos

	Controles		electrónicos.
7	Publicación matriz riesgos de seguridad digital.	Oficial de Seguridad de la Información o dependencia responsable.	Matriz riesgos de seguridad digital.
8	Tratamiento riesgos de seguridad digital.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos valoración riesgos, actas de reunión y/o correos electrónicos.
9	Monitoreo de riesgos de seguridad digital.	Procesos IDPC / Oficial de Seguridad de la Información.	Formatos valoración riesgos, actas de reunión y/o correos electrónicos.

6. CONTROL DE CAMBIOS

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
28/01/2019	01	Creación del Documento.		
28/01/2020	02	Ajuste de formato y contenido		
20/12/2021	03	Actualización del actividades para el cumplimiento de los requisitos furag	MEJORA	Requerimiento FURAG

7. CRÉDITOS

Elaboró	Revisó	Aprobó
Eusebio Cordero Orjuela Contratista - Oficial de Seguridad de la Información - Subdirección de Gestión Corporativa	Mary Rojas Contratista – Líder TI - Subdirección de Gestión Corporativa	Juan Fernando Acosta Mirkow Subdirector de Gestión Corporativa
Aprobado	Acta Comité Institucional de Gestión y Desempeño, de 31 de enero 2022	