PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CORPORACION DE CULTURA Y TURISMO DE ARMENIA

ABRIL 2019

ARMENIA QUINDIO.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

INTRODUCCION

En este documento se describe el uso y el modelo a seguir bajo el cual se va a realizar e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información dentro del Corporación de Cultura y Turismo de armenia (CCTA), en las cuales se adoptaran las mejores prácticas planteadas por Mintic en su marco de referencia de la arquitectura empresarial y de TI de gobierno en línea ahora llamado también Gobierno Digital, en su modelo de seguridad y privacidad de la información(MSPI), basándose y apoyándose en las normas y estándares de seguridad como lo son la norma iso 27005/2011.

La información que hace parte de una Entidad Pública es crucial para su correcto desempeño dentro de la política pública y su relación con el ciudadano, sin importar qué tipo de información se trate en la Entidad, ésta será parte primordial en el cumplimiento de sus Objetivos, es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de una Entidad o de un Estado.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información (MSPI), un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Por otra parte, Teniendo en cuenta que el contexto organizacional de este plan y del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa el presente plan es la “Guía de Riesgos” del DAFP, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de éste modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.(MINTIC 2016).

La Administración de riesgos en temas TI es un método sistemático que permite establecer a las entidades, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos en función de la tecnología, equipos, infraestructura etc., asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Ilustración 1 criterios de clasificación de riesgos
Fuente: tomado de (MINTIC 2016)

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Ilustración 2niveles de clasificación de riesgos
Fuente: tomado de (MINTIC 2016)

OBJETIVOS

Objetivo General

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento en la seguridad y privacidad de la información dentro de la Corporación de Cultura y Turismo de Armenia (CCTA).

Objetivos Específicos

- Concientizar a todos los funcionarios, contratistas, terceros, áreas y procesos, en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión de la entidad.
- Identificar y evaluar los riesgos dentro de la entidad.
- lograr vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información.
- orientar a la Entidad a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP.
- Involucrar y comprometer a todos los funcionarios y contratistas en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos dentro de la entidad.

DEFINICIONES

- **Administración del riesgo:** Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.
- **Activo de Información**: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Análisis de riesgos**: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
- **Amenaza:** Es la causa potencial de una situación de incidente y no deseada por la organización.
- **Causa**: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia**: Resultado de un evento que afecta los objetivos.
- **Criterios del riesgo**: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control**: Medida que modifica el riesgo.
- **Disponibilidad**: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos**: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Evento**: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.
- **Estimación del riesgo.** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Evitación del riesgo.** Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.
- **Factores de Riesgo:** Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.
- **Identificación del riesgo.** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Integridad**: Propiedad de la información relativa a su exactitud y completitud.
- **Impacto.** Cambio adverso en el nivel de los objetivos del negocio logrados.

- **Nivel de riesgo**: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.
- **Riesgo Inherente**: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.
- **Riesgo Residual**: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Riesgo**: Efecto de la incertidumbre sobre los objetivos.
- **Riesgo en la seguridad de la información.** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.
- **Reducción del riesgo.** Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento. Dentro de cualquier entidad se debe como recomendación usar el proceso para la administración del riesgo dado por el DAFP. En el cual nos enseña un contexto estratégico organizacional, mediante el cual nos guiaremos en para la identificación de los riesgos, la evaluación de ellos, su análisis y sus políticas de uso entre otros más y este lo aplicaremos a cada enfoque que se necesite en este caso para la seguridad y privacidad de la información.

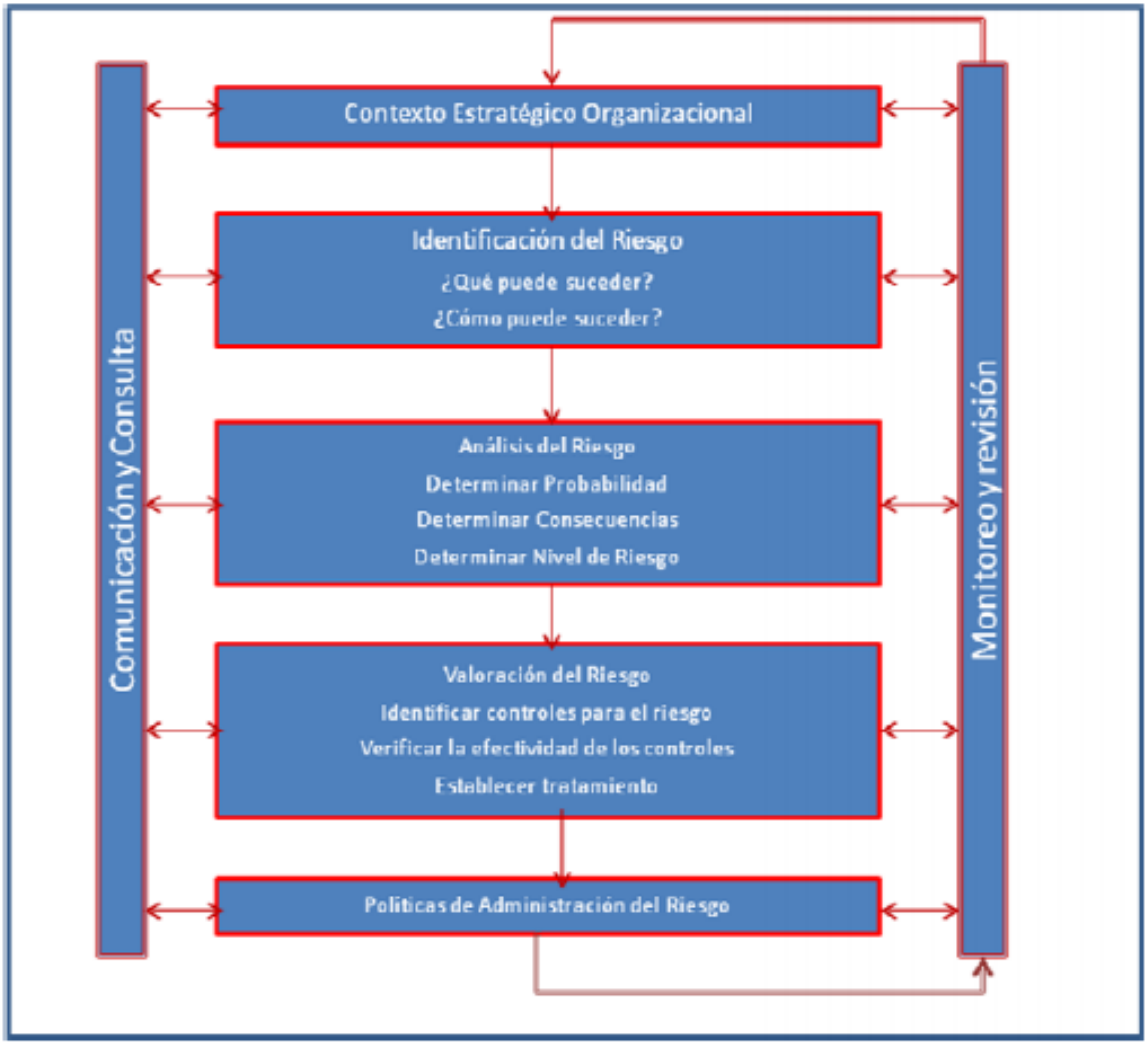

Ilustración 3Proceso para la administración del riesgo
Fuente: tomado de la cartilla de administración de riesgos de la dafp

A continuación, y en base en lo dicho anteriormente se presenta Proceso para la administración del riesgo en seguridad de la información la norma la ISO 27005.

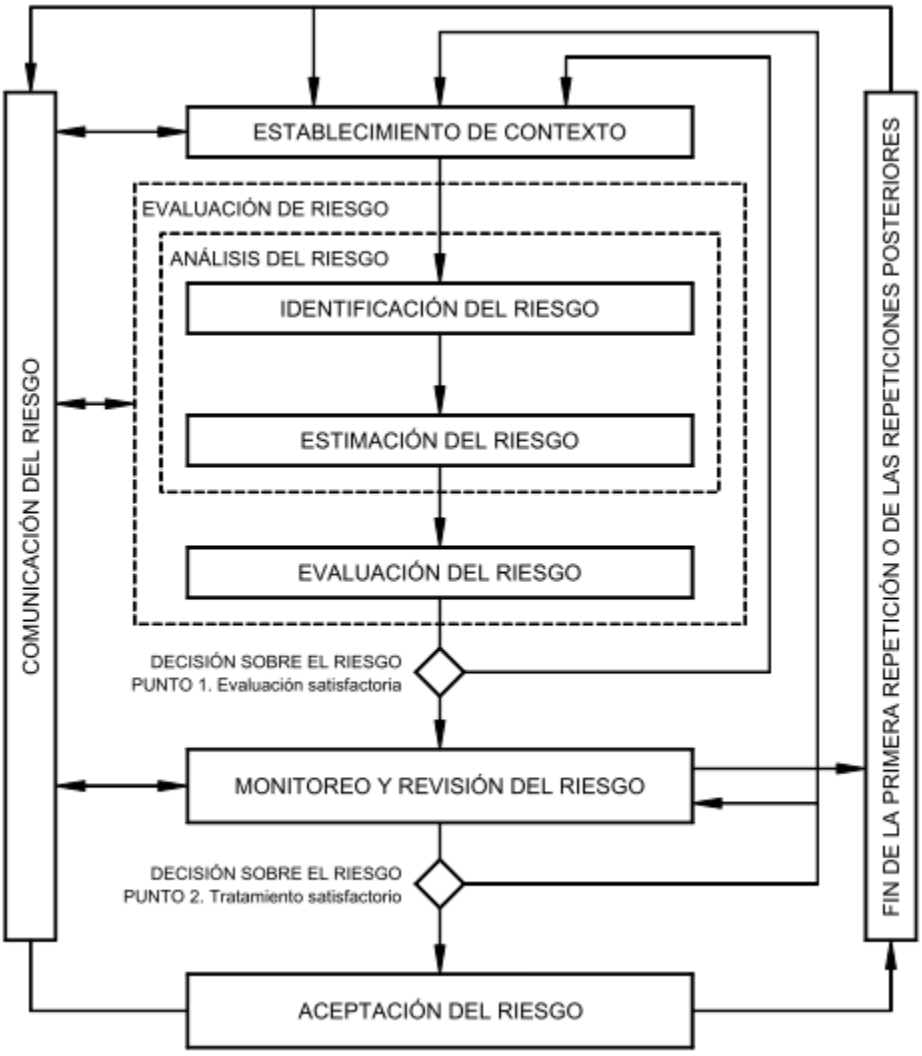

Ilustración 4 Proceso para la administración del riesgo en seguridad de la información
Fuente: Tomado de la norma iso 27005

Como se muestra en la ilustración 4 proceso para la administración del riesgo en seguridad de la información. Se dice y en base a la norma el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las

actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.

El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta. El contexto se establece primero. Luego se realiza una valoración del riesgo. Si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto), posiblemente en partes limitadas del alcance total.

El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riego con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto). La eficacia del tratamiento de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo). La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la entidad. Esto es especialmente importante en una situación en la que la

implementación de los controles se omite o se pospone, por ejemplo, por costos. Durante todo el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia por parte de los directores y el personal acerca de los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información y de los dos puntos de decisión sobre el riesgo.(ICONTEC 2009).

Se tiene La siguiente tabla la cual resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI que es muy similar a la estipulada en la norma ISO 27005, donde muestran sus etapas, pero para los procesos de SGSI.

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementar	Implementación del Plan de Tratamiento de Riesgo
Gestionar	Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Ilustración 5Etapas de la Gestión del Riesgo a lo Largo del MSPI
Fuente: tomado de G7_Gestion_de_riesgos Mintic.

La anterior ilustración nos muestra el ciclo que lleva el MSPI en el cual debemos aplicar la gestión del riesgo y sus controles a lo largo del mismo sus etapas son: Planear, en este se establece el contexto, se realiza la valoración del riesgo su planificación y tratamiento y la aceptación del mismo. Que es lo que se está realizando a lo largo de este documento, después de esto se pasa a la fase de implementación de dicho plan, cuando este esté implementado dentro de la entidad, se realiza la etapa de monitoreo y revisión continua o también llamada la fase de Gestionar en la cual se analizara que se está realizando bien y que no se está realizando bien, que cambios se debe de hacer para su correcto funcionamiento y así pasar a la etapa final que es la mejora continua en la cual se mantendrá y mejorara el proceso de la gestión del riesgo en la seguridad y privacidad de la información.

CONTEXTO ESTRATEGICO

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Dentro del contexto estratégico que se tiene en cuenta para el avance del proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la Entidad, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la Entidad, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI.(MINTIC 2016)

Es esencial determinar el propósito de la gestión del riego en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

- Dar soporte al modelo de seguridad de la información al interior de la entidad.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un plan de respuesta a incidentes.

- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- El resultado de la especificación del contexto estratégico es la especificación del criterio básicos alcance, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

Para tener más claro que es el contexto estratégico dentro de la gestión de riesgos revisaremos a guía planteada por el DAFP en la cual hablan de este tema en sus páginas 18, 19 y nos hacen una descripción especifica de esta la cual mostraremos continuación.(DAFP 2018)

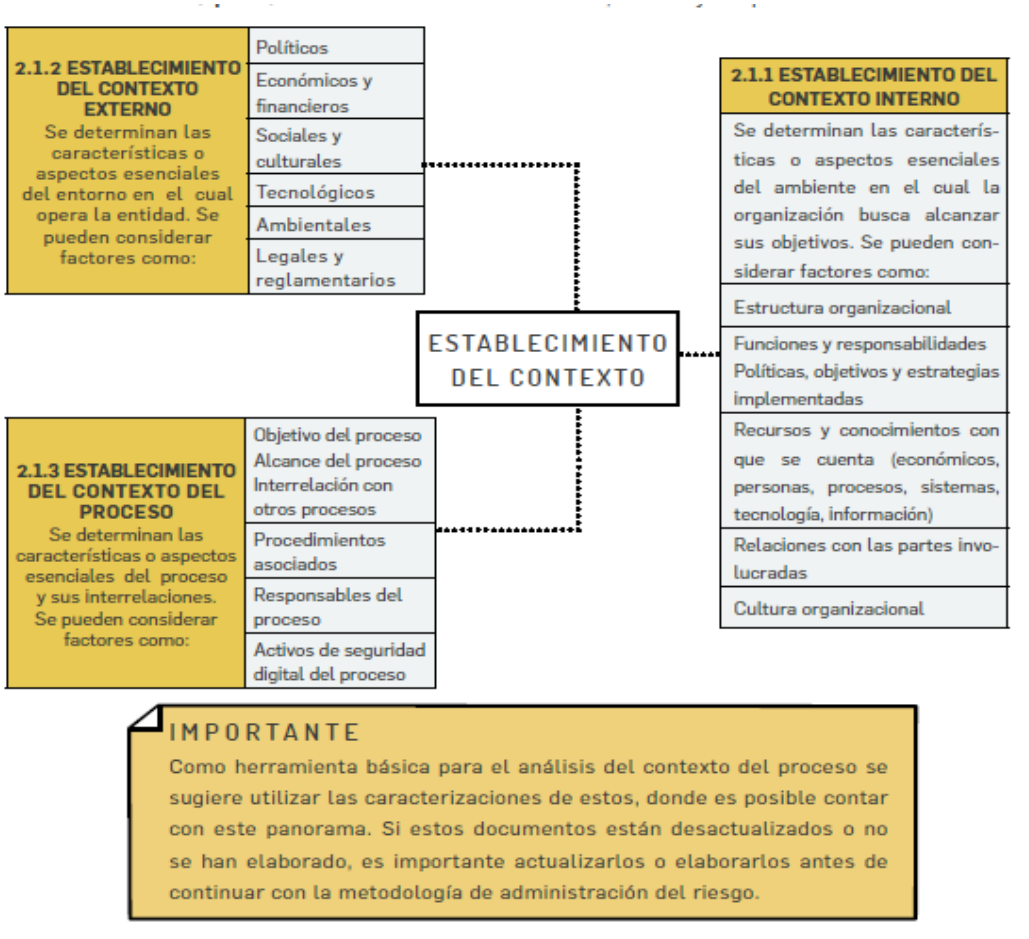

Ilustración 6 Análisis del contexto externo, interno y del proceso

Fuente: tomado de la guía para la administración de riesgos y el diseño de controles en entidades públicas DAFP

En la ilustración 6 nos muestra como el DAFP plantea el análisis del contexto estratégico, externo, interno y de proceso en la cual se deben basar las empresas para el planteamiento del mismo y como se hizo anteriormente para este plan de tratamiento de riesgos de la corporación de cultura y turismo de armenia (CTTA) y así dar avance en los siguientes puntos donde veremos los criterios de evaluación de los riesgos el alcance y sus límites para definir los riesgos dentro de la entidad en temas de seguridad y privacidad de la información.

CRITERIOS BASICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo de la Corporación de Cultura Y Turismo de Armenia (CCTA), se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo.

Criterios De Evaluación Del Riesgo

La CCTA desarrollara los criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad y privacidad de la información de la entidad, teniendo en cuenta los siguientes aspectos dentro de esta.

- El valor estratégico del proceso de información para la CCTA
- La criticidad de los activos de información involucrados en el proceso dentro de la CCTA
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la CCTA.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la CCTA.

Criterios De Impacto

La CCTA desarrollara estos criterios de impacto del riesgo y los especificara en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información de los procesos de la CCTA
- Brechas en la seguridad dela información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

Criterios De Aceptación Del Riesgo

La CCTA desarrollara y especificara estos criterios de aceptación del riesgo los cuales dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque

se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual

- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

ALCANDE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Es necesario definir el alcance del proceso de gestión del riesgo en la seguridad de la información dentro de la CCTA, con el fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

Se recolectará información acerca de la corporación de cultura y turismo de armenia para determinar el ambiente en que ella funciona y establecer la pertinencia de la información además que esto ira aliado con el PETI en su ítem gestión de información para el proceso de gestión del riesgo en la seguridad de la información y su adaptación.

La CCTA define el alcance y los límites para garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo considerando la siguiente información.

- Objetivos estratégicos de negocio, políticas y estrategias de la CCTA
- Procesos del negocio
- Funciones y estructura de la organización
- Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- La política de seguridad de la información de la organización
- El enfoque global de la organización hacia la gestión del riesgo
- Activos de información
- Ubicación de la organización y sus características geográficas
- Restricciones que afectan a la organización
- Expectativas de las partes interesadas
- Entorno sociocultural
- Interfaces (Ej. Intercambio de información con otras entidades)

ANALISIS DE RIESGOS

El análisis de riesgos dentro de la Corporación de Cultura y Turismo de Armenia (CCTA), se realiza teniendo en cuenta que para la entidad es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí la CCTA tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la Entidad decida extender el alcance de la aplicación del MSPI. A continuación, se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005.

IDENTIFICACIÓN DEL RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad, donde se mostrara más adelante en la matriz de tratamiento de riesgos.

IDENTIFICACIÓN DE LOS ACTIVOS

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software. La identificación de los activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. El nivel de detalle utilizado en la identificación de los activos tendrá influencia en la cantidad total de información recolectada durante la valoración del riesgo. Este nivel se puede mejorar en iteraciones posteriores de la valoración del riesgo.

IDENTIFICACION DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas).

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes. Con las cuales también nos guiaremos en la identificación de las nuestras.

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Contaminación	A, D, E
	Accidente Importante	A, D, E
	Destrucción del equipo o medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal funcionamiento del equipo	
	Saturación del sistema de información	
	Mal funcionamiento del software	
	Incumplimiento en el mantenimiento del sistema de información.	
Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	

	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal	

Fuente: tomado de ISO27005

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos	Ventaja competitiva Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica

extranjeros, otros intereses)		• Hurto de información • Intrusión en privacidad personal • Ingeniería social • Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Fuente: tomado de ISO27005

La CCTA realiza la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo, se deberían considerar en la misma

forma que aquellos que ya están implementados. Un control existente planificado se podría calificar como **ineficaz, insuficiente o injustificado, si es injustificado o insuficiente,** se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.
- Efectuar revisiones en sitio comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas.

IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.

La sola presencia de una vulnerabilidad no causa daño por si misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla

para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo. Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Las vulnerabilidades que se originan desde fuentes diferentes se deben considerar, por ejemplo, aquellas intrínsecas o extrínsecas al activo. A continuación, se enunciarán vulnerabilidades conocidas y métodos para la valoración de la misma.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.

	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos

	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto

	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	

ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de	Abuso de los derechos
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo

	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Fuente: basado en ISO 27005

IDENTIFICACIÓN DE LAS CONSECUENCIAS

Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc.

Esta actividad identifica los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información El impacto de los escenarios de incidente se determina tomando en consideración los criterios del impacto que se definen durante la actividad de establecimiento del contexto. Puede afectar a uno o más activos o a una parte de un activo. De este modo, los activos pueden tener valores asignados tanto para su costo financiero como por las consecuencias en el negocio, si se deterioran o se ven comprometidos. Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo.

Las organizaciones deberían identificar las consecuencias operativas de los escenarios

de incidentes en términos de (pero no limitarse a):

- tiempo de investigación y reparación;
- pérdida de tiempo (trabajo);
- pérdida de oportunidad;
- salud y seguridad;
- costo financiero de las habilidades específicas para reparar el daño;
- imagen, reputación y buen nombre.

EVALUACIÓN DE RIESGO

La CCTA debe hacer esta evaluación de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual *la guía*

presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen.

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Ilustración 7 Matriz de Calificación, Evaluación y respuesta a los Riesgos
Fuente: guía de administración de riesgos de la dafp

TABLA DE PROBABILIAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	probable	El evento probablemente ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Ilustración 8 tabla probabilidad

TABLA DE IMPACTO		
NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efecto mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto mínimos sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efecto sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Ilustración 9 tabla de impacto

PLAN DE TRATAMIENTO DE RIESGOS

Nro.	Riesgo	Clasificación de activo	Tipo de Riesgo	Causas	Probabilidad	Impacto	Riesgo Inherente		Opción de Manejo	Actividad de Control
1	Acceso no autorizado a los activos de información	Organizacion	Seguridad de la Informacion	1. Ausencia de principios y valores 2. Deficiencia o vulnerabilidades de hardware y/o software de seguridad 3. Consentimiento y/o soborno a los servidores públicos 4. Incumplimiento de las políticas o procedimientos existentes	4	2	8	Alto	Reducir o Evitar o Transferir	1. Restricción en el uso de dispositivos USB que no sean de la entidad 2. Clasificacion de la información 3. Definición de perfiles de acceso a la información 4.Cumplimiento de las Políticas de privacidad y seguridad de la información
2	Descarga, instalación y/o uso de software no autorizado.	Software	Seguridad de la Informacion	1. Multas y/o sanciones por uso ilegal de software 2. Perdida o alteración de la información de la entidad 3. Ataques informáticos 4. Indisponibilidad en los servicios TI	3	4	12	Extremo	Reducir o Evitar o Transferir	1. Restricción de descargas a través de Internet por personal no autorizado 2. Restricción a la instalación de software por personal no autorizado 3. Adquisición de software corporativo a través de procesos de contratación que garantizan que los proveedores sean canales autorizados. 4. Monitorear constantemente los equipos de computo validando que solo se tiene instalado software corporativo
3	Uso indebido o inadecuado de la información que de la entidad	Organizacion	Seguridad de la Informacion	1. Ausencia de principios y valores 2. Niveles de acceso inadecuados a la información por parte de terceros 4. Actos malintencionados de terceros (ataques informáticos) 5. Incumplimiento de las políticas o procedimientos existentes	1	3	3	Moderado	Reducir	1. Restricción en el uso de dispositivos USB que no sean de la entidad 2. Clasificación de la información 3. Definición de perfiles de acceso a la información 4. Tablas de retención documental 5.Implementar adecuadamente la ejecución de copias de seguridad a la información que permiten tener trazabilidad y posibilidad de recuperación ante la perdida de información
4	daños eventuales sobre la infraestructura física y tecnologica	Lugar	ambiental	1.Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos 2.Ubicación en área susceptible de inundación 3.Red energética inestable 4, evento natural (incendio, inundacion) 5.corto circuito en la red	2	4	8	Alto	Reducir o Evitar o Transferir	1.aplicar plan de políticas de privacidad y seguridad de la información. 2,mantenimiento de las instalaciones físicas y tecnicas de la entidad.
5	Fallas en la operación de la plataforma tecnológica (hardware y/o en el software Base)	hardware y software	Tecnologico	1.Desactualizaciones de versiones de programas informáticos 2.Obsolescencia y/o daño en los equipos 3.Manejo inadecuado y/o operación incorrecta por parte de los usuarios y técnicos 4.No renovar a tiempo las licencias o soporte	2	1	2	Bajo	Asumir	1. Se realiza mantenimiento preventivo y correctivo sobre plataforma tecnológica. 2. Se realiza monitoreo a los diferentes elementos que componen la plataforma tecnológica. 3. aplicar plan de políticas de privacidad y seguridad de la información. 4. Verificar y monitorear licencias de la entidad. de soportes y plataformas tecnologicas
6	Indisponibilidad en las telecomunicaciones (canal internet)	Red	Tecnologico	1. Daños en la infraestructura del proveedor 2. Uso inadecuado del canal de internet 3. Incumplimiento en la ejecución contractual de los proveedores. 4.Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento).	4	2	8	Alto	Reducir o Evitar o Transferir	1. Supervisión del contrato con el proveedor del servicio. 2. Monitorear el funcionamiento de las redes de voz, datos y equipos. 3. Implementar, ajustar topologías a la red de voz y datos
7	Sistemas de información adquiridos puestos en producción, que no cumplen con las ecesidades del negocio o tienen fallas	Software	Tecnologico	1.Deficiencia en las etapas de construcción de sistemas de información. 2.Deficiencia en los estudios previos. 3.errores de software en el fabricante.	2	2	4	Bajo	Asumir	1. Definición de especificaciones funcionales de acuerdo a los procedimientos establecidos. 2. Ejecución de pruebas de aceptación por el área funcional. 3. Preparación y ajuste de estudios previos para la compra de software
8	Acciones no autorizadas en el manejo del software	Software	Tecnologico	1,Uso no autorizado del equipo 2,Copia fraudulenta del software 3,Uso de software falso o copiado	1	3	3	Moderado	Reducir	1.llevar acabo plan de políticas de privacidad de la informacion. 2,verificar licencias de software
9	Ocultar a la ciudadanía información considerada pública.	Personal	Seguridad de la Informacion	1,información del portal de la corporacion desactualizado en algunas instancias. 2,información de interés publico sin acceso para los ciudadanos.	1	3	3	Moderado	Reducir	1,verificar la pagina que ntoda la informacion este publicada y de acceso publico.
10	Pérdida, robo o uso indebido de información institucional.	personal y software	Seguridad de la Informacion	1,Ataques informáticos. 2.Virus. 3,Personas.	3	4	12	Extremo	Reducir o Evitar o Transferir	1,Realización copias de Seguridad de la información. 2,Actualización de Hardware y Software de Seguridad. 3. Socialización y sensibilización a los servidores públicos.

Ilustración 10 Tratamiento de Riesgos

En la anterior ilustración en la tabla de tratamiento de riesgos de la corporación de Cultura y Turismo de armenia se muestra el riesgo establecido en la entidad, cuáles son sus causas además tipo de riesgo clasificación de activos, su probabilidad y su impacto para así realizarse la evaluación del riesgo saber que acción tomar según la guía de administración del riesgo del DAFP. Establecer actividades de control sus probabilidades e impacto nuevamente de estos controles para saber que avance se va teniendo en estos controles, quienes serían los responsables y con que periocidad se realizara a partir de su implementación.

Se anexa el hipervínculo con el Excel detallado de la matriz donde se encontrará más completa y se verá la forma en que se realizó la evaluación del riesgo de la seguridad y privacidad de la información de la corporación de cultura y turismo de armenia.

tratamiento de Riesgos ppsi2019.xlsx

link página web

http://www.armeniaculturayturismo.gov.co/planes-programas-proyectos

Bibliografía

DAFP. 2018. “Guía Para La Administración de Los Riesgos de Gestión , Corrupción y Seguridad Digital y El Diseño de Controles En Entidades Públicas.” : 94. http://www.funcionpublica.gov.co/documents/418548/34150781/Guía+para+la+Administración+de+los+Riesgos+de+Gestión%2C+Corrupción+y+Seguridad+Digital+y+el+Diseño+de+Controles+en+Entidades+Públicas+-+Agosto+de+2018.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?dow.

ICONTEC. 2009. “Ntc Iso 27005.” *Icontec*: 10.

MINTIC. 2016. “Guía de Gestión de Riesgos.” *Mintic* (7): 39. http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf.