MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN UN ESCENARIO DEL POSCONFLICTO EN COLOMBIA

DIGITAL SECURITY RISK MANAGEMENT MODEL IN A POST-CONFLICT SCENARIO IN COLOMBIA

Henry Numpaque Gambasica [1]
Jennifer Ospina Castañeda [2]

Resumen

Este artículo tiene como objetivo central, presentar un ejemplo de aplicación del modelo de gestión de riesgos de seguridad digital para el órgano de la Jurisdicción Especial para la Paz (JEP), que se encuentra enmarcado en un escenario del posconflicto en Colombia, posterior a la firma del acuerdo final de paz. Con el fin de desarrollar este artículo reflexivo, se recopila información del evento *Bsides Colombia 2019*, ciclos de conferencias enmarcados en "*La Seguridad soy ¡YO! 9.0"* -organizado por la Presidencia de la República- y el análisis de algunos documentos relacionados con la seguridad digital. Finalizado el ejercicio de aplicación, este documento muestra parte de los resultados del tratamiento de la gestión de riesgos de seguridad en la JEP, con el fin de concientizar a todos los gestores de los sistemas de información, comunicaciones o servicios informáticos acerca de la importancia del correcto manejo de los activos de información en la Entidad.

Palabras clave: ciberdefensa, ciberseguridad, seguridad de la información, seguridad digital, tecnología, JEP.

Abstract

The main objective of this article is to present an example of the application of the digital security risk management model for the Special Jurisdiction for Peace (SJP), which is framed in a post-conflict scenario in Colombia, after the signing of the final peace agreement. In order to develop this reflective article, information is collected from the Bsides Colombia 2019 event, conference cycles framed in "La Seguridad soy ¡YO! 9.0" -organized by the Presidency of the Republic- and the analysis of some documents related to digital security. At the end of the application exercise, this document shows part of the results of the treatment of security risk management in the SJP, in order to make all managers of information systems, communications or computer services aware of the importance of the correct management of information assets in the Entity.

Keywords: cyber defense, cybersecurity, information security, digital security, technology, SJP.

Recepción: Septiembre de 2021 / Evaluación: Octubre de 2021 / Aprobado: Diciembre de 2021

1 Tecnólogo en sistematización de Datos, Universidad Distrital Francisco Jose De Caldas, Desarrollado de plataformas, Bogotá, Colombia, https://orcid.org/0000-0002-3861-4548 correo hengua@gmail.com

[2] Tecnólogo en sistematización de Datos, Universidad Distrital Francisco Jose De Caldas, Gestor de procesos en áreas TI., Bogotá, Colombia, https://orcid.org/0000-0003-3874-6804 correo producc.academicaud@gmail.com

Introducción

En los últimos años el mundo ha sido testigo de una revolución tecnológica, así como del uso masivo de las tecnologías de la información y las comunicaciones (TIC), facilitando el desarrollo de las actividades de las entidades públicas y privadas. Paralelamente a estos escenarios, hay un aumento de los riesgos para la seguridad digital asociados a los activos de información que soportan la operación de las organizaciones. La gestión de riesgos que es un conjunto de procesos -secuencia de tareas- y procedimientos -descripción detallada de cómo se debe llevar a cabo un proceso- interminables, busca proteger el activo más importante de una entidad: la información. Por esta razón los gobiernos han creado mecanismos para identificar, analizar, evaluar y tratar el riesgo de seguridad digital, así como para seleccionar medidas preventivas y correctivas de seguridad de la información.

Dentro de las principales metodologías de análisis de riesgos se encuentra el método armonizado de análisis de riesgos (MEHARI), la Expresión de necesidades e Identificación de los Objetivos de Seguridad (EBIOS), Evaluación de vulnerabilidades, activos y amenazas operativamente críticas (OCTAVE), Análisis práctico de amenazas (PTA) y el método de la Oficina Federal de Seguridad en Tecnologías de la Información de Alemania (BSI). (La seguridad informática en la PYME, 2016, p. 46)

Otros autores como Javier Areitio sugieren una metodología general para desarrollar una política de seguridad basada en "cinco fases interrelacionadas: Análisis y valoración de riesgos, construcción de la política, implantación de la política, mantenimiento de la política e implicación de todo el componente humano". (Seguridad de la información, 2008, p. 43)

Según el Ministerio de Tecnologías de la Información y las Comunicaciones (2021) con período de corte al tercer trimestre del año 2020, Colombia registraba 7,67 millones de accesos fijos a internet a nivel nacional, lo que conlleva a la necesidad de contar con herramientas de seguridad para contrarrestar el incremento de las amenazas informáticas que afecten significativamente al país, razón por la cual el MinTIC ha puesto en marcha diversas estrategias como "la Política para Ciberseguridad y Ciberdefensa (CONPES 3701 y 3854), un modelo de seguridad y privacidad de la información (MSPI) y misiones de asistencia técnica internacional". (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017, p. 8)

Dentro de esas estrategias, el MinTIC creó el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) en el cual se pueden reconocer las amenazas y vulnerabilidades informáticas a las que una entidad pueda estar expuesta con el fin de fortalecer principios de la seguridad de la información (confidencialidad, integridad y disponibilidad), promoviendo así un ambiente de control, generando confianza, e impulsando la prosperidad económica y social de la entidad y, por consiguiente, del país.

Metodología

La idea de escribir este artículo surge de la falta de conciencia que aún existe en Colombia acerca de la importancia de la seguridad de la información. El desarrollo se expone basado en la metodología hipotético-deductiva, a través de la observación, hipótesis, deducción y comprobación de los resultados.

La etapa de observación se realiza a través del estudio de ataques cibernéticos importantes a entidades gubernamentales, se analiza el impacto económico relacionado con los ataques

cibernéticos y se hace una síntesis del Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD).

Para la hipótesis, se seleccionaron 5 activos de la información de la JEP para determinar el nivel de criticidad e identificar amenazas, vulnerabilidades y riesgos de estos.

La deducción se da por la probabilidad de ocurrencia y el impacto con el fin de determinar la zona en la que se encuentra el riesgo inherente asociado a cada activo de información.

Finalmente, se plantean los resultados a través de una serie de controles que permita la gestión de riesgos digitales en la entidad de la JEP.

- **Observación**

Esta etapa expone una revisión de ataques cibernéticos en entidades gubernamentales, impacto en la economía y la fase de planificación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital.

Revisión Ataques cibernéticos

Un informe del Centro Cibernético Policial (2020) señala que para el año 2020 se registraron 35.184 denuncias sobre incidentes cibernéticos, es decir un 82% más que el año 2019. Otro informe de la misma entidad reveló que las entidades gubernamentales fueron objeto de ataques informáticos a través de "puertas traseras" gracias a la infección de malware y la utilización de RAT (Remote Access Tool) para la ejecución de software malicioso que sirve para la transferencia ilegal y no consentida de dinero, información del sector público y bases de datos. (Centro Cibernético Policial, 2017, p. 4)

Como antecedentes recientes de ataques a entidades del Estado, el 26 de noviembre de 2019 la cuenta de Twitter @judicaturacsj_ fue hackeada y se publicaron varios trinos ofensivos hacia el presidente Iván Duque (El Tiempo, 2019).

Figura 1. Tweets de la @judicatura. Fuente: ElTiempo.com

El 26 de septiembre del mismo año, la JEP -Jurisdicción Especial para la Paz-, fue objeto de un ataque cibernético en la seguridad de su página web "que afectó el centro de almacenamiento de datos de la entidad". (Semana, 2019)

Impacto económico de las amenazas para la seguridad digital

Un estudio elaborado por la Organización de Estados Americanos y el Ministerio de Tecnologías de la Información y las Comunicaciones (2017) señaló que:

Con respecto al daño a los activos e infraestructura de la entidad, más de 40% de las entidades tuvieron un costo más pequeño que COP $ 1.000.001, 20% tuvieron un costo entre COP $ 1.000.001 – COP $ 15.000.000, y aproximadamente 20% entre COP $ 15.000.001 – COP $ 235.000.000. Sin embargo, cerca de 17% de las entidades presentaron costos relativos a daño a activos de más de 700 millones de pesos colombianos en 2016. (p.93)

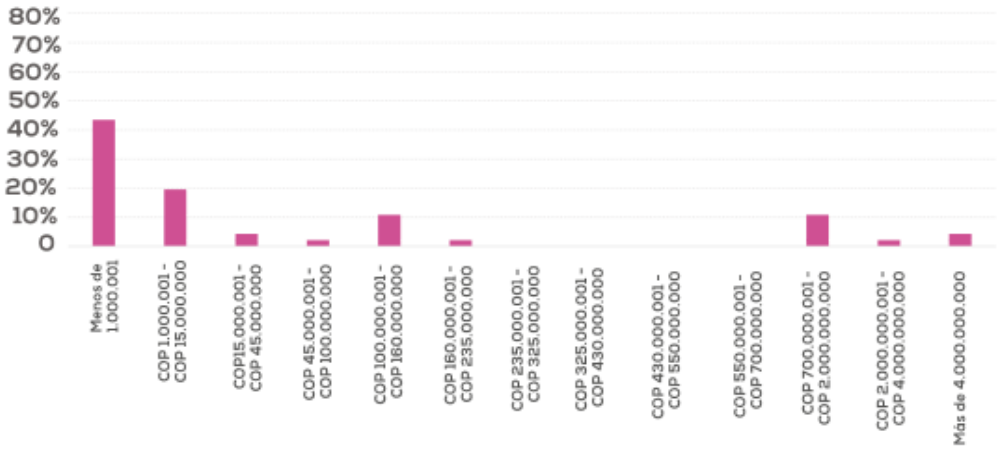

Figura 2. Costos de daños a los activos e infraestructura incurridos por las entidades estatales que estimaron el impacto de los incidentes digitales 2016. Fuente: Organización de Estados Americanos y el Ministerio de Tecnologías de la Información y las Comunicaciones (2017)

Modelo Nacional de Gestión de Riesgos de Seguridad Digital

Dentro de las estrategias del Gobierno Nacional para enfrentar las amenazas informáticas, se encuentra el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD), "basado en buenas prácticas nacionales e internacionales para la gestión de riesgos y tiene como fin contribuir a la prosperidad económica y social, por medio de acciones que conlleven al aprovechamiento de un entorno digital seguro". (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017, p. 9)

El marco conceptual de este modelo"provee una guía para la implementación de gestión de riesgos de seguridad digital basado en principios generales y fundamentales donde se establece una interacción con los Sistemas de Gestión de la Seguridad de la Información (SGSI) o para el caso de las entidades del sector público colombiano con el Modelo de Privacidad y Seguridad de la Información (MPSI); así como la relación con los activos de información que soportan la operación de cualquier Entidad u Organización a nivel general y en particular con las denominadas infraestructuras Criticas Cibernéticas por el CCOC". (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017, p. 37)

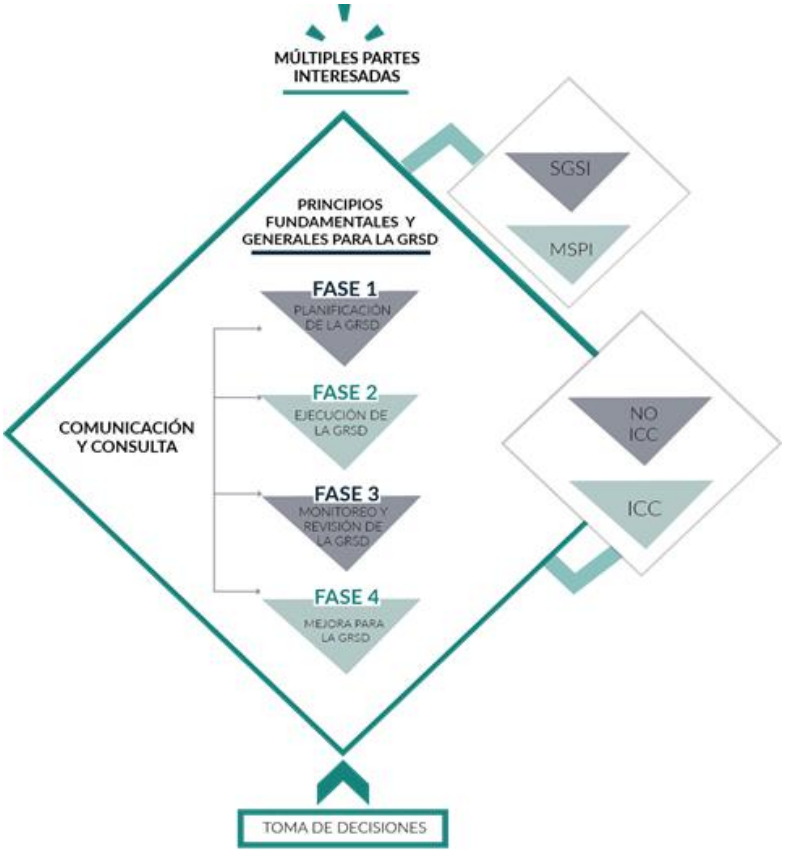

Figura 3. Marco conceptual del Modelo de Gestión de Riesgos de Seguridad Digital. Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Ejemplo de aplicación del Modelo de Gestión de Riesgos de Seguridad Digital

Con el fin de aplicar este modelo y teniendo en cuenta los ataques cibernéticos e informes sobre el impacto de las amenazas mencionados anteriormente, se decidió tomar como objeto de estudio, la Jurisdicción Especial para la Paz (JEP).

La JEP en su proceso de adopción de la Política de Seguridad y Privacidad de la Información (MSPI) mediante el acuerdo AOG N°045 de 2019 identifica que "El alcance del SGSPI, son los activos de información requeridos para el adecuado funcionamiento de todos los procesos de la Jurisdicción Especial para la Paz, en la sede central, grupos territoriales y en las demás que en el futuro se establezcan". (Jurisdicción Especial para la Paz, 2019, p. 11)

Por lo anterior y para este ejemplo, se describen algunas de las fases que hacen parte de la Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público.

- **Planificación de la GRSD**

Establecimiento del contexto

La JEP, tiene como misión "administrar justicia para consolidar la transición hacia la paz y restaurar el tejido social, garantizando los derechos de las víctimas y la seguridad jurídica de los comparecientes, con enfoque territorial, diferencial y de género". (Jurisdicción Especial para la Paz, 2018)

Como visión es "a 2033 haber hecho justicia, esclareciendo y estableciendo las responsabilidades penales individuales sobre los crímenes más graves y representativos cometidos durante el conflicto armado colombiano y resolviendo la situación jurídica de todos los comparecientes a la JEP, contribuyendo así a la construcción de la paz y la reconciliación nacional". (Jurisdicción Especial para la Paz, 2018)

Identificación de partes interesadas

"Se identifican víctimas, comparecientes de la ex guerrilla de las Farc, de la Fuerza Pública, de agentes del estado, de la protesta social y de terceros civiles, así como el público en general, servidores públicos de la JEP, contratistas, comunidad internacional, entidades concernidas, medios de comunicación y otras entidades del Estado". (Jurisdicción Especial para la Paz, 2019, p. 7)

Definición de roles y responsabilidades (Jurisdicción Especial para la Paz, 2019, p. 13)

- Órgano de Gobierno, encargado de la aprobación de la Política General de la Seguridad de la Información.
- Secretaría Ejecutiva, encargada de la formulación y presentación para aprobación por parte del Órgano de Gobierno.
- Comité de Seguridad de la Información, responsable del seguimiento de la aplicación de la Política de la Seguridad de la Información para el SGSPI -Sistema de Gestión de Seguridad y Privacidad de la Información-.
- Dirección de Tecnologías de la Información, responsable de la planeación, coordinación y administración del SGSPI.
- Oficial de Seguridad de la Información, responsable de apoyar a la Dirección de TI.
- Comité de Seguridad Informática de la JEP, que aprobará el manual de SGSPI.

Criterios para la gestión del riesgo de seguridad digital

Se exponen los criterios de impacto en confidencialidad, integridad, disponibilidad, social, económico y ambienta

Tabla 1. *Criterios de impacto de seguridad de la información de la JEP*

Valoración asignada	Valor asignado	Criterios de impacto de seguridad de la información					
		Integridad	**Disponibilidad**	**Confidencialidad**	**Social**	**Económica**	**Ambiental**
Insignificante	1	Sin afectación	Sin afectación	Sin afectación	Afectación del 0,1% de la población o menos	Afectación del 0,1% del presupuesto de la Entidad o menos	Sin afectación medioambiental
Menor	2	Afectación muy leve	Afectación muy leve	Afectación muy leve	Afectación del 0,2% de la población o menos	Afectación del 0,2% del presupuesto de la Entidad	Afectación muy leve del m.a. que requiere de 6 meses de recuperación
Moderado	3	Afectación leve	Afectación leve	Afectación leve	Afectación del 0,3% de la población o menos	Afectación del 0,3% del presupuesto de la Entidad	Afectación leve del m.a. que requiere 1 año de recuperación
Mayor	4	Afectación grave	Afectación grave	Afectación grave	Afectación del 0,4% de la población o menos	Afectación del 0,4% del presupuesto de la Entidad	Afectación leve del m.a. que requiere 2 años de recuperación
Catastrófico	5	Afectación muy grave	Afectación muy grave	Afectación muy grave	Afectación del 0,5% de la población o menos	Afectación del 0,5% del presupuesto de la Entidad	Afectación leve del m.a. que requiere 3 años de recuperación

Nota: Elaborado por el autor

Criterios de probabilidad

Se consideran 5 niveles de la siguiente manera:

Tabla 2. *Valoración de probabilidad de ocurrencia de la JEP*

Valoración asignada	Valor asignado	Frecuencia	Posibilidad
Raro	1	La situación se ha presentado al menos cada 10 años	La situación podría suceder al menos cada 10 años
Improbable	2	La situación se ha presentado al menos una vez cada año	La situación podría suceder al menos una vez cada año
Posible	3	La situación se ha presentado al menos una vez cada semestre	La situación podría suceder al menos una vez cada semestre
Probable	4	La situación se ha presentado al menos una vez al mes	La situación podría suceder al menos una vez al mes
Casi seguro	5	La situación se ha presentado al menos una vez a la semana	La situación podría suceder al menos una vez a la semana

Nota: Elaborado por el autor

Definición del Nivel o Zona de Riesgo

Se proponen las siguientes zonas:

Tabla 3. *Zona de riesgos de acuerdo a la combinación de impacto y probabilidad*

Zona de riesgo	Valor asignado	Acción requerida
Extremo	Mayor o igual que 15	Requiere acciones inmediatas para evitar la materialización de los riesgos asociados a los activos de información.
Alto	Mayor o igual a 9 y menor de 15	Requiere de acciones rápidas por parte de la Alta Dirección para disminuir el riesgo de seguridad digital.
Moderado	Mayor o igual a 4 y menor de 9	Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo de seguridad digital a niveles inferiores del actual.
Bajo	Menor de 3	El riesgo de seguridad digital se mitiga con actividades propias de la Entidad y por medio de acciones detectivas y correctivas.

Nota: Elaborado por el autor

Definición de Apetito de Riesgo o Zona de Riesgo Aceptable:

Para este ejemplo se define que el apetito de riesgo de la Entidad estará enmarcado en la zona de riesgos bajos.

- **Hipótesis**

Ejecución de la GRSD

Identificación de activos de información

Se seleccionan 5 activos de la JEP se realiza el siguiente análisis:

Tabla 4. *Clasificación de los activos de información de la JEP*

No. activo	Nombre del activo	Subprocesos - Procedimientos	Dueño del riesgo sobre el activo	Responsable del activo	Clasificación del activo
A1	Portal web	Comunicaciones	JEP	Comunicaciones	software
A2	Redes sociales	Comunicaciones	JEP	Comunicaciones	software
A3	Orfeo	Gestión Documental	JEP	Gestión Documental	software
A4	Equipos de cómputo	Tecnologías de la Información	JEP	Tecnologías de la Información	hardware
A5	Datacenter	Tecnologías de la información	JEP	Tecnologías de la Información	Instalaciones

Nota: Elaborado por el autor

Determinar nivel de criticidad del activo

Se plantean una serie de preguntas con las opciones de respuesta SI o NO, a las cuáles se les asigna un valor, donde SI equivale a 0,1 y NO equivale a 0,0.

El nivel de importancia del activo se da por los siguientes intervalos:

- Menos de 0,45 será de importancia baja.
- Entre 0,45 y 0,75 será de importancia media.
- Mayor a 0,75 será de importancia alta.

Tabla 5. *Nivel de importancia de los activos de información de la JEP*

No. del activo		A1	A2	A3	A4	A5
Nombre del activo		Portal web	Redes sociales	Orfeo	Equipos de cómputo	Datacenter
¿El activo pertenece a terceros?		No	No	No	No	No
		0,0	0,0	0,0	0,0	0,0
¿El activo debe ser restringido a un número de usuarios?		Si	Si	Si	Si	Si
		0,1	0,1	0,1	0,1	0,1
¿El activo es muy crítico para las operaciones internas?		Si	Si	Si	Si	Si
		0,1	0,1	0,1	0,1	0,1
¿El activo es muy crítico para el servicio a terceros?		Si	Si	Si	No	Si
		0,1	0,1	0,1	0,1	0,1
¿En caso de ser utilizado o modificado por alguna persona o sistema sin la debida utilización, afectaría negativamente los sistemas y/o procesos de manera:	**Leve (0,2)**					
	Importante (0,3)		X			
			0,3			
	Grave (0,5)	X		x	X	X
		0,5		0,5	0,5	0,5
Criticidad		0,8	0,6	0,8	0,8	0,8
Nivel de importancia del activo		Alta	Media	Alta	Alta	Alta

Nota: elaborado por el autor

Identificación de ICC (Infraestructura Crítica Cibernética)

Analizados los criterios anteriores, se determina que la JEP tiene identificada su ICC puesto que una falla en el datacenter, en el software de gestión documental 'Orfeo' o en el portal web, podría afectar la consulta de información pública de la entidad, así como la generación de peticiones, quejas o reclamos de los usuarios en caso de colapso de los activos mencionados.

Clasificación de la información

Se realiza la clasificación de la información de acuerdo con:

- La Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional según la Ley 1712 de 2014 (Artículo 6).
- Los criterios horizontales de criticidad para establecer si una infraestructura estratégica cibernética es una ICC, de acuerdo con la Guía de Infraestructura Crítica Cibernética para Colombia de la Asociación Colombiana de Ingenieros de Sistemas -ACIS- (2016).
- La Guía para la Gestión y Clasificación de Activos de Información del Ministerio de Tecnologías de la Información y las Comunicaciones (2016).

Se definen los siguientes criterios para establecer si una infraestructura estratégica (IEC) es una infraestructura crítica cibernética (ICC):

1. El impacto social: Valorado en función de la afectación de la población (incluyendo pérdida de vidas humanas), el sufrimiento físico y la alteración de la vida cotidiana. Valorado en función de la población total colombiana: 49.827.269 de habitantes. Fuente: DANE
2. El impacto económico Valorado en la magnitud de las pérdidas económicas en relación con el Producto Interno Bruto de Colombia (PIB). 377.739.622.866
3. Impacto Medioambiental: Valorado en función de los años que tarda la recuperación del medio ambiente.

Analizados los criterios anteriores, se determina que la JEP cuenta con Infraestructura Crítica Cibernética (ICC), pues en caso de materializarse fallas en el los activos identificados podrían afectar la gestión de procesos relacionados con administración de justicia transicional y conocimiento de los delitos cometidos en el marco del conflicto armado que se hubieran cometido antes del 1 de diciembre de 2016, así como a los usuarios internos y externos de sus aplicaciones lo cual puede desencadenar quejas por parte de los usuarios del portal web y beneficiarios del software de gestión documental.

Tabla 6. *Identificación de ICC y clasificación de la información de la JEP.*

No. activo	Nombre del activo	Nivel de criticidad del activo	ICC				Clasificación de la información
			Social	Económico	Ambiental	Se debe reportar	
A1	Portal web	Alta	x	x		Debe reportar al CCOC	Información pública
A2	Redes sociales	Media	x			Debe reportar al CCOC	Información pública

A3	Orfeo	Alta		x		Debe reportar al CCOC	Información pública clasificada
A4	Equipos de cómputo	Alta				Debe reportar al CCOC	Información pública reservada
A5	Datacenter	Alta	x	x		No debe reportar al CCOC	Información pública reservada

Nota: elaborado por el autor

- **Deducción**

Identificación de riesgos de seguridad digital (Incluye riesgos de las ICC)

Una vez identificados los activos críticos y clasificados, se procede a identificar las amenazas y vulnerabilidades de cada uno de los activos. Para el presente ejemplo, se identifica un riesgo por activo.

Tabla 7. *Amenazas, vulnerabilidades y riesgos de los activos de información y las ICC de la JEP*

No. activo	**Nombre del activo**	**Clasificación del activo**	**# riesgo**	**Amenaza**	**Vulnerabilidades**	**Riesgo**
A1	Portal web	Software	R1	Hackeo no ético	Credenciales débiles	Defacement de la página web
A2	Redes sociales	Software	R2	Botnets	Credenciales débiles	Phishing
A3	Orfeo	Software	R3	Datos incompletos	Falta de validaciones	Error en la información
A4	Equipos de cómputo	Hardware	R4	Empleados o terceros	Exceso de confianza	Robo de información
A5	Datacenter	Instalaciones	R5	Empleados de la entidad	Control de acceso físico	Acceso físico no autorizado

Nota: elaborado por el autor

Seguidamente, se calcula la probabilidad de ocurrencia y el impacto para determinar la zona en la que se encuentra ubicado el riesgo inherente asociado a cada activo de información o crítico.

Tabla 8. *Matriz de riesgos inherentes*

# Riesgo	Riesgo	Probabilidad de ocurrencia	Social	Económico	Ambiental	Confidencialidad	Integridad	Disponibilidad	Nivel de riesgo
R1	Defacement de la página web	4-Probable	4-Mayor	1-Insignificante		1-Insignificante	5-Catastrófico	5-Catastrófico	13-Alta
R2	Phishing	4-Probable	1-Insignificante	1-Insignificante		1-Insignificante	5-Catastrófico	1-Insignificante	7-Alta
R3	Error en la información	5-Casi seguro	3-Moderado	1-Insignificante		1-Insignificante	3-Moderado	1-Insignificante	9-Alta
R4	Robo de información	5-Casi seguro	3-Moderado	1-Insignificante		5-Catastrófico	5-Catastrófico	5-Catastrófico	19-Extremo
R5	Acceso físico no autorizado	1-Raro	5-Catastrófico	5-Catastrófico		5-Catastrófico	5-Catastrófico	5-Catastrófico	5-Alta

Nota: elaborado por el autor

Estos valores permiten tener los riesgos inherentes y se puede determinar el mapa de calor donde se identifica la posición de cada uno de los riesgos en matriz:

IMPACTO	**5-Catastrófico**	R5				
	4-Mayor					R4
	3-Moderado				R1	
	2-Menor				R2	R3
	1-Insignificante					
		1-Raro	**2-Improbable**	**3-Posible**	**4-Probable**	**5-Casi seguro**
	PROBABILIDAD					

Resultados

Para el presente artículo, se suponen los siguientes controles para los riesgos inherentes:

Tabla 9. *Matriz de controles identificados asociados a cada riesgo - JEP*

Activo	**# riesgo**	**Riesgo**	**Control**
Página web	R1	Defacement de la página web	Certificado SSL
Redes sociales	R2	Phishing	Gestión de contraseñas
Orfeo	R3	Error en la información	Validación de datos de entrada
Equipos de cómputo	R4	Robo de información	Procedimientos de registro de inicio seguro
Datacenter	R5	Acceso físico no autorizado	Tarjetas de control

Nota: Elaborado por el autor

Determinación del riesgo residual

Teniendo en cuenta los valores de la 'tabla 14 - Análisis y evaluación de controles' de la Guía para la Orientación de la GRSD en el Gobierno Nacional, y para el presente artículo se evalúan los controles R1, R2 y R4.

Tabla 10. *Evaluación de los controles asociados a cada riesgo - JEP*

Criterios de evaluación	Consideración de variables	Evaluación de control (R1): Certificado SSL	Evaluación de control (R2): Gestión de Contraseñas	Evaluación de control (R4): Procedimientos de registro de inicio seguro
Categoría del control	Estratégico=1 Táctico=2 Operativo=3	1	3	1
Naturaleza del control	Manual=1 Mixto=2 Automático=3	3	1	3
Documentación	Si existe=1 No existe=0	1	0	1
Complejidad	Complejo para ejecutar=1 No complejo=0	0	0	0
Responsable del control	Asignado=1 No asignado=0	1	0	1

Tipo de control	Preventivo=3 Detectivo=2 Correctivo=1	3	3	3
Importancia sobre la mitigación del riesgo	Si=1 No=0	1	0	1
Puede disminuir la probabilidad	Si=1 No=0	1	1	1
Puede disminuir el impacto	Si=1 No=0	1	1	1
	Total	**12**	**9**	**12**

Nota: Elaborado por el autor

Teniendo la sección de rango de calificación de los controles de la Guía para la Orientación de la GRSD en el Gobierno Nacional, y los resultados de los controles se establece que:

Para los controles, *Certificado SSL* (R1) y *Procedimientos de registro de inicio seguro* (R4), cuyo resultado fue 12, se consideran como controles muy efectivos y dado que el resultado de la característica "*puede disminuir la probabilidad*" es igual a uno, estos controles se desplazan en probabilidad a la izquierda dos cuadrantes y hacia abajo, dos cuadrantes ya que la característica "*puede disminuir el impacto*".es igual a uno.

Para el control *Gestión de contraseñas* (R2) cuyo resultado fue de 9, se considera como efectivo y se desplaza la probabilidad a la izquierda un cuadrante ya que la característica "puede disminuir la probabilidad" es igual a uno, y hacia abajo un cuadrante ya a que la característica "*puede disminuir el impacto*" es igual a uno.

Al final los riesgos residuales quedan ubicados en el mapa de calor de la siguiente manera:

IMPACTO	**5-Catastrófico**	R5				
	4-Mayor					
	3-Moderado					
	2-Menor			**R4**		R3
	1-Insignificante		**R1**	**R2**		
		1-Raro	**2-Improbable**	**3-Posible**	**4-Probable**	**5-Casi seguro**
	PROBABILIDAD					

Tratamiento de los riesgos de seguridad digital

Luego de evaluados los riesgos de seguridad digital, se muestran los tres riesgos analizados y su respectivo tratamiento.

Tabla 11. *Tratamiento de los riesgos de seguridad digital - JEP*

Tratamiento de los riesgos			
Riesgo	R1	R2	R4
Activo de información	Página web	Redes sociales	Equipos de cómputo
Riesgo	Defacement de la página web	Phishing	Robo de información
Nivel de riesgo residual	Zona de riesgo baja	Zona de riesgo baja	Zona de riesgo alta
Plan de tratamiento	Asumir el riesgo	Asumir el riesgo	Reducir el riesgo, evitar, compartir o transferir
Descripción del tratamiento	-Debido a que la página web se encuentra en la red interna de la Entidad, se han de incorporar elementos de protección perimetral para protegerlo. -Ubicar el servidor web en una zona desmilitarizada -DMZ-, evitando así que un intruso pueda acceder a la red interna si vulnera el servidor web.	Robustecer protocolos de seguridad con el fin de contrarrestar situaciones que pongan en riesgo la disponibilidad, integridad y la confidencialidad de la información.	Robustecer los protocolos de seguridad, realizar monitoreo constante de las acciones realizadas por los usuarios, y actualizar a las últimas versiones y parches de seguridad.
Área responsable	Tecnologías de la Información	Comunicaciones	Tecnologías de la Información
Responsable del proceso	Jefe de Tecnologías de la Información	Jefe de Comunicaciones	Jefe de Tecnologías de la Información
Fecha de inicio de la ejecución	A convenir	A convenir	A convenir
Fecha de fin de la ejecución	A convenir	A convenir	A convenir

Para terminar y de acuerdo con el numeral 4.3.1 de la Guía para la Orientación de la GRSD en el Gobierno Nacional, se debe hacer seguimiento a estos planes de tratamiento.

Conclusiones

Tras la implementación del modelo de gestión de riesgos de seguridad digital para el órgano de la JEP, se puede concluir que, a través de la aplicación de buenas prácticas y teniendo en cuenta la importancia que tiene la información de esta entidad dentro de su entorno digital, se puede aumentar la eficiencia, confianza y seguridad en la prestación de los servicios a los ciudadanos, así como el fortalecimiento del manejo y seguridad de los activos de información de la Entidad.

Los mecanismos para la identificación, análisis, evaluación, tratamiento de riesgos y controles de seguridad en una entidad pública o privada pueden garantizar la disminución de la probabilidad e impacto en caso de que algún activo de la información pueda sufrir algún riesgo.

Así mismo, este artículo permite concluir que es necesario orientar a la ciudadanía sobre el uso responsable del medio digital con el fin de no comprometer la información en su confidencialidad, integridad y disponibilidad.

Referencias bibliográficas

Alcaldía de Envigado (2007). ISO 27002. Recuperado de: http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001070&ruta=/documentacion/0000001358/0000000107

Areitio Bertolin, Javier (2008). Seguridad de la información: Redes, informática y sistemas de información. Recuperado de: https://books.google.com.co/books?id=_z2GcBD3deYC&printsec=frontcover&dq=%22gesti%C3%B3n+de+riesgos%22+%22seguridad+digital%22&hl=es&sa=X&ved=2ahUKEwjknJmLurj3AhUelmoFHd5dAtI4FBDoAXoECAoQAg#v=onepage&q&f=false

Asobancaria (2018). La gestión de la ciberseguridad: un asunto de supervivencia para las organizaciones. Recuperado de: https://www.asobancaria.com/wp-content/uploads/1133-C-23-04-2018.pdf

Asociación Colombiana de Ingenieros de Sistemas -ACIS- (2016). Infraestructura Crítica Cibernética. Recuperado de: https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Banco Interamericano de Desarrollo -BID- (2017). Impacto de los incidentes de seguridad digital en Colombia 2017. Recuperado de: https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

Carpentier, Jean-Francois (2016). La seguridad en la informática en la PYME: Situación actual y mejores prácticas. Recuperado de: https://books.google.com.co/books?id=LKE5_6gzBmgC&printsec=frontcover&dq=%22gesti%C3%B3n+de+riesgos%22+%22seguridad+digital%22&hl=es&sa=X&ved=2ahUKEwjknJmLurj3AhUelmoFHd5dAtI4FBDoAXoECAgQAg#v=onepage&q&f=false

Centro Cibernético Policial. (2017). Informe: Balance Cibercrimen en Colombia 2017. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.pdf

Centro Cibernético Policial. (2019). Tendencias del Cibercrimen en Colombia 2019-2020. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

Centro Cibernético Policial. (2020). Balance Cibercrimen 2020. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_201217_1_1_0.p df

Comando Conjunto Cibernético (2017). Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PNPICCN V 1.0. Recuperado de: https://www.ccoc.mil.co/recursos_user///PLAN_PUBLICO.pdf

Departamento Nacional de Planeación (2011). Documento Conpes 3701 - Lineamientos de política para ciberseguridad y ciberdefensa. Recuperado de: https://tic.bogota.gov.co/sites/default/files/marcolegal/CONPES%203701%20DE%202011.pdf

Departamento Nacional de Planeación (2017). Documento Conpes 3854 - Política Nacional de Seguridad Digital. Recuperado de: https://tic.bogota.gov.co/sites/default/files/marco-legal/CONPES%203701%20DE%202011.pdf

Documentos Tics (2011). Convenio sobre cibercriminalidad. Recuperado de: http://documentostics.com/documentos/convenio_cibercriminalidad.pdf

El Tiempo. (26 de noviembre de 2019). Judicatura denuncia 'hackeo' de su cuenta de Twitter. Recuperado de: https://www.eltiempo.com/justicia/cortes/judicatura-denuncia-hackeo-de-su-cuenta-de-twitter-437598

Escuela Superior de Guerra (2019). La seguridad en el ciberespacio: un desafío para Colombia. Recuperado de https://esdeguelibros.edu.co/index.php/editorial/catalog/download/42/48/741-1

Función Pública (2014). Ley 1712 de 2014. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=56882

Función Pública (2018). Modelo de Gestión de Riesgos de Seguridad Digital: Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Recuperado de:https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Función Pública (2020). Guía para la administración del riesgo y el diseño de controles en públicas. Recuperado de: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la++administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87

Gobierno Digital. (2018). Cómo se integra el MSPI a los servicios digitales de confianza y calidad. Recuperado de: https://estrategia.gobiernoenlinea.gov.co/623/articles-74968_recurso_16.pdf

Instituto Distrital de Turismo de Bogotá (2006). ISO 27001. Recuperado de: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Jurisdicción Especial para la Paz (2018). Misión, visión, funciones y deberes. Recuperado de: https://www.jep.gov.co/Paginas/mision-vision-funciones-y-deberes.aspx.

Jurisdicción Especial para la Paz (2019). Justicia más digital en la JEP. Recuperado de: https://www.jep.gov.co/organosgobierno/Acuerdo%20AOG%20No%20045%20de%202019.pdf.

Jurisdicción Especial para la Paz (2019). Política de Seguridad y Privacidad de la Información. Recuperado de: https://www.jep.gov.co/organosgobierno/Acuerdo%20AOG%20%20de%202019.pdf.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía para la Gestión y Clasificación de Activos de Información. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Instructivo para el Diligenciamiento de la Herramienta de Diagnóstico de Seguridad y Privacidad de la Información. Recuperado de: https://www.sigep.gov.co/eva/admon/files/empresas/ZW1wcmVzYV83Ng==/imagenes/4495/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. Recuperado de: https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). Modelo Nacional de Gestión de Riesgos de Seguridad Digital. Recuperado de: https://www.mintic.gov.co/portal/715/articles-61854_documento.docx

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021). Boletín trimestral de las TIC - enero de 2021. Recuperado de: https://colombiatic.mintic.gov.co/679/articles-161478_archivo_pdf.pdf

Presidencia de la República de Colombia (2018). Ley 1928: Convenio sobre la ciberdelincuencia. Recuperado de: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

Organización de los Estados Americanos. (2017). Impactos de los incidentes de seguridad digital. Recuperado de: https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf

Semana. (26 de septiembre de 2019). Ataque cibernético a la JEP. Recuperado de: https://www.semana.com/confidenciales-semanacom/articulo/ataque-cibernetico-a-la-jep/633533

Urna de Cristal. (2017). Ejemplo de aplicación del modelo de gestión de riesgos de seguridad digital. Recuperado de: https://www.urnadecristal.gov.co/sites/default/files/EJEMPLO%20APLICACIO%cc%81N%20DEL%20MGRSD.PDF

Urna de Cristal. (2017). Ejemplo de aplicación del modelo de gestión de riesgos de seguridad digital. Recuperado de: https://www.urnadecristal.gov.co/sites/default/files/Guia%20para%20la%20orientacio%C

C%81n%20de%20la%20GRSD%20en%20el%20Gobierno%20Nacional%20Entes%20Territoriales%20y%20Sector%20Publico..pdf