La justicia es de todos

Minjusticia

EVALUACIÓN Y VERIFICACIÓN AL PROCESO ASOCIADO CON LA SEGURIDAD DE LA INFORMACIÓN

Oficina de Control Interno

(2020)

1. **Objetivo de la auditoría:**

   Evaluar y verificar el estado actual del Modelo de Seguridad y Privacidad de la Información del Ministerio de Justicia y del Derecho.

2. **Alcance de la auditoría:**

   En el marco del objetivo definido, se evaluará el avance en la implementación del Modelo de Seguridad y Privacidad de la Información del MJD hasta el año en curso.

3. **Criterios de auditoría o parámetros normativos:**

   Para el desarrollo de la presente auditoría se tomarán en cuenta los siguientes criterios: Guía de Gestión de Riesgos proveída por el Modelo de Seguridad dentro de la estrategia de Gobierno en Línea; Ley 1581 de 2012; Decreto 1078 de 2015; Ley 1712 de 2014, en su artículo 18; articulo 77 de la Ley 1474 de 2011 y la norma ISO 27001.

4. **Metodología:**

   La metodología empleada por la Oficina de Control Interno, se basó en un levantamiento de información básica para la fase de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Justicia y del Derecho (MJD). A continuación, se relacionan las actividades realizadas en el marco de la auditoría.

   - **Apertura de la auditoría:** En reunión del 23 de septiembre de 2020 con el personal de Tecnología se dio apertura a la auditoría, informando el alcance y las fechas de las actividades principales.

   - **Solicitud de información relacionada con el Modelo de Seguridad y Privacidad de la Información:** El 23 de septiembre de 2020, se solicitó la información asociada al Modelo de seguridad y Privacidad de la Información. A continuación se detalla la información que fue solicitada y recibida.

N°	INFORMACIÓN SOLICITADA	RECIBIDA
1	Confirmación de los procesos y procedimientos de la Entidad sobre seguridad de la información.	✓
2	Política de seguridad de la información, formalizada y firmada.	✓
3	Organigrama, roles y responsabilidades de seguridad de la	✓

	información, asignación del recurso humano y comunicación de roles y responsabilidades.	
4	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.	✓
5	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección.	✓
6	Objetivo, alcance y límites del Modelo de Seguridad y Privacidad de la Información (MSPI).	✓
7	Documento que identifique la metodología de clasificación de activos de información.	✓
8	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección.	✓
9	Documento formalizado de la metodología de gestión de riesgos y la aceptación de los riesgos residuales por parte de los dueños de los riesgos.	✓
10	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad.	✓
11	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	✓
12	Soportes de las campañas de sensibilización y/o capacitaciones de seguridad de la información.	✓
13	Diagrama de red de la Entidad. Especificar las soluciones de seguridad en la red implementadas (por ejemplo IPS, Firewall, IDS, etc.)	✓
14	Descripción de cómo se está implementado la seguridad de la información en la gestión de proyectos.	✓
15	Inventario de partes externas o terceros a los que se transfiere información de la entidad y relación de los controles definidos para asegurar la confidencialidad e integridad de la información.	✓
16	Formato de acuerdo de transferencia de información.	✓
17	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden. Indicar, si dentro de los contratos con los proveedores se tienen definidas cláusulas de confidencialidad de la información.	✓
18	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses. Así mismo, procedimiento de gestión de incidentes vulnerabilidad y amenazas.	✓
19	Confirmación si se ha realizado pruebas de penetración o ethical hacking. En caso de haber adelantado estas pruebas, enviar los informes de los resultados de las últimas pruebas realizadas, y confirmar que periodicidad se tiene definida para la ejecución de estas pruebas.	✓

20	Plan de continuidad de la Entidad aprobado.	✓
21	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información.	✓
22	Indicadores y métricas de seguridad de la información definidos.	✓
23	Diligenciar y remitir el formato adjunto correspondiente a la carta de representación.	✓

- **Reunión para aclaración de dudas de la información solicitada:** El 13 de noviembre de 2020, se llevó a cabo la reunión de aclaración de dudas, respecto a la información solicitada, que fue expuesta por la unidad auditable en OneDrive (En la nube) ya que se presentaba una confusión con la numeración de las carpetas, las cuales están relacionadas con el cuestionario solicitado en la comunicación y apertura de la auditoría, si bien al principio se ofreció información incompleta, la reunión permitió superar dicha circunstancia.

- **Solicitud de Información adicional:** El 13 de noviembre de 2020, se solicitó en la reunión de "aclaraciones y dudas", información adicional respecto al diligenciamiento de las matrices de seguridad de la información por parte de las dependencias del MJD, fundamentales para la evaluación y desempeño de la auditoría.

- **Encuesta al grupo operativo de seguridad de la información:** El 13 de noviembre de 2020, por medio de la herramienta Teams, se realizó una breve encuesta a las personas encargadas de la seguridad de la información del área de tecnología, y en especial, a la oficial de seguridad de la información.

5. Desarrollo de la Auditoría:

Teniendo bajo consideración el objetivo de la presente auditoría, es pertinente ofrecer una breve alusión al concepto de seguridad de la Información, sobre el cual el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece que "*El Modelo de Seguridad y Privacidad de la Información (MSPI), conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.*"

Dicho modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte del MJD, que permita fijar los criterios que

servirán para proteger la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Teniendo en cuenta lo anterior, se desarrolló la auditoría con base en los aspectos cruciales para promover dicho proceso al interior de la entidad, y que se citan a continuación:

5.1 Documento de la política de seguridad y privacidad de la Información

Con el fin de preservar la información del Ministerio de Justicia y del Derecho (MJD), garantizando la integridad, confidencialidad y disponibilidad de la misma, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales, sus procesos misionales, y que este adaptada a las condiciones específicas y particulares de cada una según corresponda, para que sea aprobada y guiada por la Dirección, como lo aconseja el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC), en su guía #2 "*Elaboración de la política general de seguridad y privacidad de la información",* como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

Se verifica y se constata que el MJD cuenta con el documento de la Política de Seguridad de la Información. Se evalúa el documento encontrando que:

- El documento de la política de seguridad de la información cuenta con los objetivos y alcance definidos.

- El objetivo de la política de seguridad de la información se encuentra alineado con la estrategia y objetivos del MJD.

- Fue revisada y aprobada por la anterior administración ¿a través o por intermedio? de la subdirección y dirección de tecnologías de la información.

- La política contiene la definición del concepto de seguridad de la información.

- Establece la asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a través de roles definidos.

- La responsable designada por la Dirección de Tecnología para desarrollar, actualizar y revisar las políticas es la Ingeniera "Liliana Rodríguez Prieto".

No obstante lo anterior, desde ya es importante que la función sea asignada a un cargo específico, y no a un nombre en especial, con el fin de promover la continuidad de dicho servicio, en caso de que la persona que figura actualmente se desvincule. También es necesario que en ausencias temporales del servidor, se prevea qué cargo ha de suplir el liderazgo en torno al tema.

- La política se revisa una vez por año, dependiendo de las necesidades que se detecten; para la presente vigencia, se contempla incluir los dominios faltantes.

- La Dirección de Tecnología Gestión e Información en Justicia (DTGIJ), viene adelantando la nueva actualización de la política de seguridad de la información, la cual tiene como última fecha de emisión el 6 de agosto del 2018.

5.2 Políticas de Seguridad y Privacidad de la Información.

La Dirección de Tecnología y Gestión de Información en Justicia (DTGIJ), define sus políticas en dos documentos que son: Política de la Seguridad de la Información y Política de Tecnologías de la Información, esta última no se encuentra publicada en el SIG, por lo cual, desde ya, se hace un llamado para ello. Analizando las políticas que se definen en estos documentos encontramos que carece de políticas específicas que promuevan la implementación de controles de Seguridad de la Información.

La guía N° 2 "*Elaboración de la política general de seguridad y privacidad de la información."* del Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), presenta algunas recomendaciones de políticas de seguridad de la información. Este conjunto de recomendaciones no es obligatorio, ya que estas se generan de acuerdo a las necesidades o sus características particulares, sus activos de información, sus procesos y los servicios de información; a continuación, se mencionarán las políticas recomendadas en la guía con el objetivo de hacer una implementación transversal de Seguridad de la Información en el MJD:

- **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:** Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información.

- **NO REPUDIO:** La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

- **PRIVACIDAD Y CONFIDENCIALIDAD:** Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente.

- **INTEGRIDAD:** La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información.

- **REGISTRO Y AUDITORÍA:** Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

- **CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN:** Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Mencionado lo anterior, se recomienda en la actualización de la política de seguridad de la información, la cual se encuentra en desarrollo, incluir las políticas recomendadas por la guía N° 2 “Elaboración de la política general de seguridad y privacidad de la información.” del Modelo de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

5.3 Roles y responsabilidades para la seguridad de la información

La guía del Modelo de Seguridad y Privacidad de la Información (MSPI) establece que la entidad debe definir mediante un acto administrativo (Resolución, circular, Decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, de procesos y operativos) que permitan la correcta toma de decisiones y una adecuada gestión al cumplimiento de los objetivos de la Entidad.

Se valida y se encuentra que, el MJD define mediante el documento de la política de seguridad de la información, roles y responsabilidades de seguridad de la información en diferentes niveles como:

- ✓ Comité institucional de gestión y desempeño.

- ✓ Personal directivo.

- ✓ Comité operativo de seguridad de la información.
- ✓ Oficial de seguridad de la información.
- ✓ Líder de seguridad informática.
- ✓ Subdirección de tecnologías y sistemas de información.
- ✓ Servidores públicos del Ministerio de Justicia y del Derecho.

Dado lo anterior, en el desarrollo de la presente auditoría, se evidenciaron las siguientes no conformidades en cuanto a roles y responsabilidades para la seguridad de la información:

- ➢ El documento de la política de seguridad de la información no contempla los roles y responsabilidades de los proveedores.
- ➢ No están claramente definidos los roles y responsabilidades en cuanto a la asignación de personal con las competencias requeridas.

5.3.1 Equipo del Modelo de Seguridad y Privacidad de la Información.

Es preciso aclarar, que no solo deben estar definidos los roles en los diferentes niveles del MJD, pues deben estar definidos los roles que se tendrán establecidos en las tareas que realizará cada uno de los miembros del equipo del Modelo de Seguridad y Privacidad de la Información (MSPI). Partiendo de este punto, el MJD tendrá asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable. A continuación se realizan algunas recomendaciones que ofrece la guía N°4 “Roles y Responsabilidades” del MSPI del MinTic:

“Se debe organizar un grupo de trabajo responsable para implementar el MSPI en el MJD, con el fin de poder realizar la labor de la manera más eficiente, se sugiere un conjunto de integrantes para el equipo al interior del MJD, denominados de la siguiente forma:

- ➢ ***Un responsable de Seguridad de la Información para el MJD**: El cual ya se encuentra definido por la DTGIJ.*
- ➢ ***Equipo del Proyecto:** debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la*

información más relevante del MJD esté disponible oportunamente. De manera general, se pone a consideración el siguiente listado, el cual recomienda la guía N°4 de "Roles y Responsabilidades" del MSPI del MinTic, para que las entidades analicen -de acuerdo a su composición orgánica-, cuáles deben ser los miembros del equipo de seguridad y privacidad de la información, teniendo en cuenta los siguientes perfiles:

- ✓ *Personal de seguridad de la información.*
- ✓ *Un representante del área de Tecnología.*
- ✓ *Un representante del área de Control Interno.*
- ✓ *Un representante del área de Planeación.*
- ✓ *Un representante de sistemas de Gestión de Calidad.*
- ✓ *Un representante del área Jurídica.*
- ✓ *Funcionarios, proveedores y ciudadanos."*

La siguiente imagen presenta los perfiles de manera genérica, y el nivel al cual pertenecerían según lo propuesto:

Imagen de la Guía N°4 de Roles y responsabilidades de MinTic

De esta forma se busca asegurar que sea una iniciativa de carácter transversal al MJD y que no dependa exclusivamente de la Dirección de Tecnología y Gestión de Información en Justicia.

- **Comité de seguridad:** Se encuentra definido en el MJD, pero si este necesita ser restructurado, se recomienda la plantilla de la guía de roles y responsabilidades que podría servir como base para la generación de la resolución para la creación del comité de seguridad de la información.

5.4 Contacto con las autoridades

Las entidades deben tener procedimientos establecidos que especifiquen cuándo, y a través de qué, se debe contactar a las autoridades, y cómo se deben reportar de una manera oportuna los incidentes de seguridad de la información identificados.

Se analiza la información allegada por la DTGIJ encontrando que, se viene adelantando el documento “Régimen Sancionatorio”, en el cual, el MJD contemple las sanciones por el uso indebido de los activos de información, con el fin de reducir la ocurrencia de malas prácticas.

Las sanciones se aplicarán a los usuarios que incurran en delitos informáticos o en incumplimiento a las políticas o lineamientos de seguridad de la información o en conductas que afecten la integridad, disponibilidad y confidencialidad de la información del MJD. El documento será de interés interno, aplicable a funcionarios, contratistas, y terceros autorizados a nivel nacional; se aclara que aún no se encuentra aprobado.

La Subdirección de Tecnologías y Sistemas de Información viene adelantando campañas de sensibilización vía correos institucionales, señalando las sanciones con pena de prisión por incumplimientos de ley.

Pese a que se está elaborando el documento “Régimen Sancionatorio”, se recomienda terminarlo lo más pronto, el cual sea aprobado y publicado en el SIG.

5.5 Contacto con grupos de interés especiales

Como buenas practicas, se deben mantener contactos apropiados con grupos de interés especial, u otros como foros y asociaciones profesionales especializadas en seguridad.

De las evidencias presentadas se observa que la DTGIJ, socializa la “Política Nacional de Confianza y Seguridad Digital” del Consejo Nacional de Política Económica y Social (CONPES), la cual fue trabajada por el Departamento Nacional de Planeación, Ministerio de Tecnología de la información y las Comunicaciones y el Departamento Administrativo de la Presidencia de la República, teniendo como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital en Colombia, y que fue socializada al interior de la DTGIJ por su director.

A su vez, se participó dando respuesta a la información solicitada por el consejero presidencial para asuntos económicos y transformación digital de la

Presidencia de la República, con el diagnóstico de ciudadanía digital, ciberseguridad, ciberdefensa y ciberdelincuencia.

Si bien la Dirección de Tecnología y Gestión de Información en Justicia (DTGIJ), viene adelantando participación con organismos profesionales y especializados, se recomienda establecer contactos de interés con stakeholders que no sean del estado.

5.6 Inventarios de Activos de información

La guía N° 5 Gestión y Clasificación de Activos de MinTic señala que, "*la realización de un inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad,* cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A, del estándar ISO/IEC 27001:2013. A continuación se mencionan los cuatro puntos principales:

> ***Inventario de activos:*** *todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de los mismos.*
>
> ***Propiedad de los activos:*** *los activos de información del inventario deben tener un propietario.*
>
> ***Clasificación de la información:*** *La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.*
>
> ***Etiquetado y manipulado de la información:*** *Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización."*

Siguiendo los 4 puntos recomendados en el Modelo de Seguridad y Privacidad de la Información (MSPI), se valida la información allegada para el desarrollo de la presente auditoría, encontrando que la DTGIJ se encuentra actualizando los instrumentos de gestión, para las cuales realizaron las siguientes actividades:

- ✓ Definición de grupo líder vía memorando (DJ-DTGIJ-GGD).
- ✓ Lanzamiento de piezas publicitarias, promoviendo el próximo inventario.

- ✓ Citación a líderes de transparencia vía correo electrónico a mesa informativa e instructiva.

- ✓ Socialización a todas las dependencias del cronograma de trabajo, formato de inventario, acta de aprobación a través de mesa de trabajo.

- ✓ Envió de material necesario para actualización y revisión por parte de los líderes de cada dependencia con fecha límite de entrega (por EPX para dar oficialidad).

- ✓ Asesoramiento por parte del equipo líder a las dependencias.

- ✓ Revisión por parte del equipo líder y consolidación.

- ✓ Aprobación y firma de actas por parte de jefes de cada dependencia.

- ✓ Extracción para definir Instrumentos de Gestión de Información Ley 1712 de 2014.

- ✓ Registro, Índice, Esquema (web master).

- ✓ Validación de acto administrativo – concepto jurídico.

- ✓ Se encuentra Publicado en link de transparencia – página web del MJD.

5.6.1 Resultados encontrados tras la actualización de los instrumentos de gestión.

Posterior a la identificación de los activos de información se identifican los principios de seguridad relacionados con la información (Confidencialidad, integridad y disponibilidad).

5.6.1.1 El principio de confidencialidad se valora cuando:

Si un individuo, entidad o proceso no autorizado accede al activo, conoce su información, parametrización o configuración, esto puede afectar la operación de la Entidad, generando un incumplimiento normativo.

Alta: Detectado por entes de control externos, pérdida reputación a nivel nacional o internacional. Podría generar una pérdida económica significativa en multas, demandas, sanciones o reprocesos.

Media: Detectado por entes de control internos, pérdida reputación a nivel nacional. Podría generar una pérdida económica moderada en multas, demandas, sanciones o reprocesos.

Baja: Si un individuo, entidad o proceso no autorizado accede al activo, conoce su información, parametrización o configuración, esto puede afectar la operación de la Entidad, generando un incumplimiento normativo, riesgo de pérdida reputación o podría generar pérdida en reprocesos.

5.6.1.2 El principio de integridad se valora cuando:

Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen.

Alta: Severas de la entidad.

Media: Moderado a funcionarios de la entidad.

Baja: Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

5.6.1.3 El principio de disponibilidad se valora cuando:

La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen.

Alta: Severas a entes externos.

Media: Moderado de la entidad.

Baja: La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

5.6.1.4. Conclusiones sobre la aplicación de los principios y estado de los activos de información:

De las 26 dependencias que diligenciaron la matriz de activos de información, falta por entregar el grupo de Asuntos Legislativos, al igual que el grupo de Gestión Contractual; a este último, le falta clasificar un activo de información.

DEPENDENCIA	CRITICIDAD		
	ALTO	MEDIO	BAJO
CID	0	4	0
SST	7	5	0
GAIT	9	2	0
SEA	1	3	0
VPJ	0	2	1
DMASC	34	16	1
SGIJ	0	4	18
SCYFSQ	6	2	0
OAP	0	0	17
APRENSAC	8	0	0
OCI	10	0	0
GSC	0	13	7
GGD	8	0	0
GGH	5	10	0
GGC	0	17	0
GGAFYC	25	1	0
GAIYT	0	11	0
DPDYAR	2	6	0
DPCYP	5	13	16
DJF	1	21	0
DJT	4	11	1
DJ	0	16	16
DAI	12	3	0
DDOJ	2	22	0
SG	0	2	11
GAL	Sin Entregar	Sin Entregar	Sin Entregar

Se concluye que, del 100% del inventario de activos de información, el cual se encuentra en actualización tiene un avance del 92%. A su vez, de manera relevante el inventario define el propietario del activo, custodio del activo, se valora el activo de información bajo el criterio de la Ley 1581, tipo de clasificación

y por último el respaldo de información, verificando que se cumple con los principios y estado de los activos de información.

5.7 Proceso disciplinario

El Ministerio de Justicia y del Derecho (MJD), debe contar con un proceso disciplinario formal[1], el cual debe ser comunicado para emprender acciones contra funcionarios y contratistas que hayan cometido una violación a la seguridad de la información.

Validando la información allegada por el auditado, se evidencia que se tiene el documento de “Régimen Sancionatorio”, el cual aún no se encuentra aprobado. Cabe resaltar, que el documento abarca de manera muy completa las sanciones al uso indebido de los activos de información del MJD, a continuación se menciona el objetivo y alcance del documento.

> ***OBJETIVO***
>
> *Definir las acciones orientadas a sancionar el uso indebido de los activos información del Ministerio de Justicia y del Derecho; por medio de tablas de auditoría, reportes de los sistemas de información, alertas de seguridad y/o testigos, con el fin de reducir la ocurrencia de malas prácticas.*
>
> ***ALCANCE***
>
> *Documento de interés interno, aplicable a funcionarios, contratistas, y terceros autorizados, a nivel nacional. Las sanciones se aplicarán a los usuarios que incurran en delitos informáticos o en incumplimiento a las políticas o lineamientos de seguridad de la información o en conductas que afecten la integridad, disponibilidad y confidencialidad de la información de Ministerio de Justicia y del Derecho.*

A su vez, la DTGIJ informa periódicamente a través del correo institucional los diferentes incumplimientos por delitos en la seguridad de la información.

Se recomienda finalizar y publicar el documento lo más pronto, para ser socializado al interior del MJD, para que este sea del interés de funcionarios y contratistas, y así controlar las violaciones a la seguridad de la información.

5.8 Plan de Comunicaciones

[1] Se hace alusión a un proceso que defina las reglas, sanciones y comportamientos disciplinables frente a la seguridad de la información, sin perjuicio del régimen disciplinario de la Ley 734 de 2002.

El Ministerio de Justicia y del Derecho (MJD), debe definir un plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del MJD.

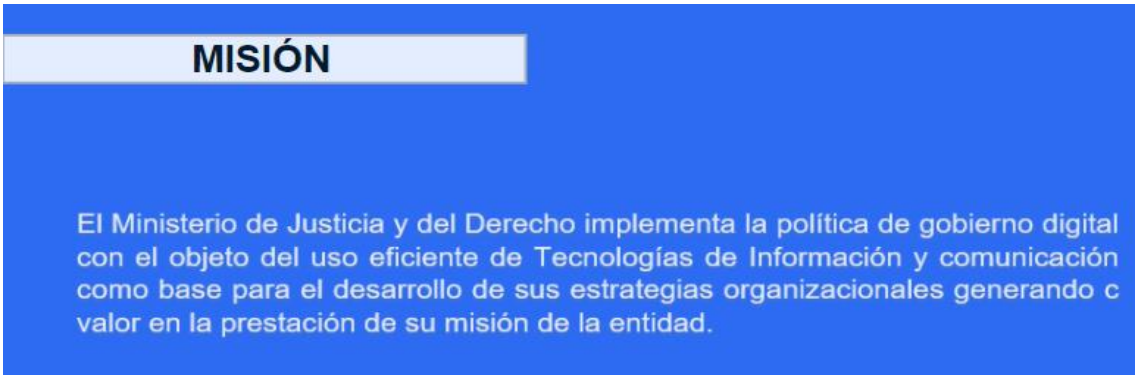
Por lo anterior, el modelo de seguridad y privacidad de la información indica: "*pautas específicas para guiar a las instituciones a robustecer sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de una Entidad.*

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información."

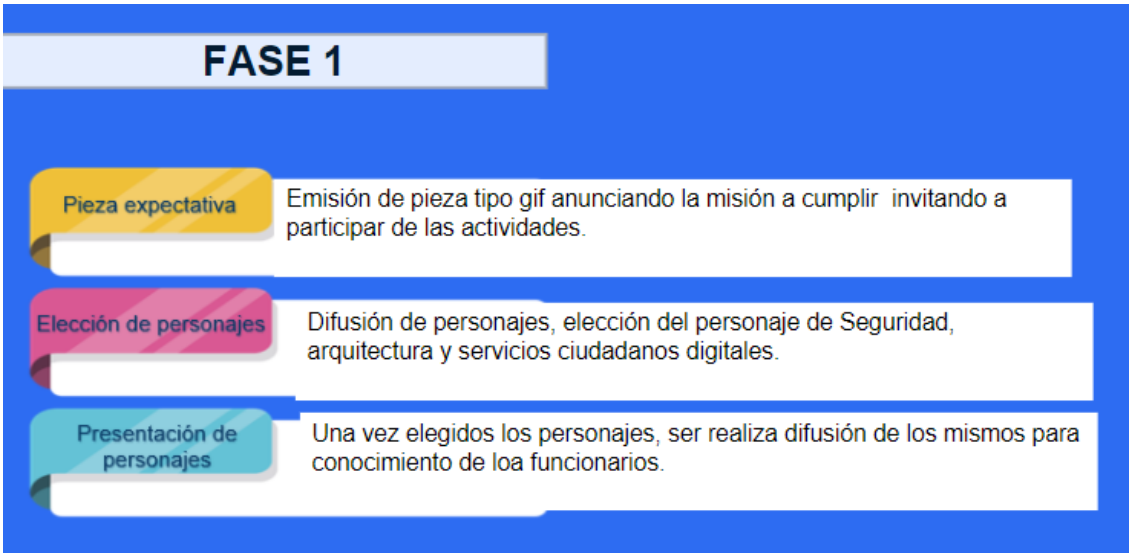
Una vez analizada la información entregada por la unidad auditada (OneDrive Carpeta #11) se evidenció que la DTGIJ, realizó la propuesta al "Uso y Apropiación para Gobierno Digital y Habilitadores", fortaleciéndolo con el contrato 0438 de 2020, suscrito por la Nación – Ministerio de Justicia y del Derecho y ALGOAP INC S.A.S, el cual contempla el siguiente objeto contractual, *"Implementar la estrategia de uso y apropiación de las TIC para el personal funcional del Ministerio de Justicia y desarrollar capacitación y formación en Tecnología de la Información para la Dirección de Tecnologías y Gestión de Información en Justicia (DTGIJ)",* a continuación se detallan las fases de la estrategia realizada.

PLAN DE SENSIBILIZACIÓN DE GOBIERNO DIGITAL, SEGURIDAD Y SERVICIOS CIUDADANOS DIGITALES						
FASE	EJE TRANSVERSAL	NOMBRE DE LA ACTIVIDAD	DESCRIPCIÓN DE LA ACTIVIDAD	MEDIOS DE DIFUS	FECHA DE SOCIAL	RECURSOS
FASE I DE EXPECTATIVA - ELECCIÓN DE PERSONAJES	ARQUITECTURA, SEGURIDAD SERVICIOS	DISEÑO DE PERSONAJES Y VALIDACIÓN	Se realiza el diseño de los personajes de Arquitectura, seguridad y servicios ciudadanos digitales, se presenta al equipo de uso y apropiación líderes de estas tematicas y se aprueban	Presentación a través de teams	24/09/2020	*Personajes digitales * Equipo de uso y apropiación
	ARQUITECTURA, SEGURIDAD SERVICIOS	PIEZA EXPECTATIVA	Se enviara pieza expectativa invitando hacer parte de la misión " El Ministerio de Justicia y del Derecho implementa la política de gobierno digital con el objeto del uso eficiente de Tecnologías de Información y comunicación como base para el desarrollo de sus estrategias organizacionales generando valor en la prestación de su misión de la	Mailing-intranet	29/09/2020	* Material de expectativa * Equipo de uso y apropiación * Funcionarios y contratistas del Ministerio de Justicia y del Derecho
	ARQUITECTURA, SEGURIDAD SERVICIOS	ELECCIÓN DE PERSONAJES	Se creara un formulario en Forms donde se integre la misión, el nombre de los personajes , caracteristicas y los personajes con el fin de que los funcionarios y contratistas elijan el personaje que quieren elegir.	Mailing-intranet	1/10/2020	* Formulario * Equipo de uso y apropiación * Funcionarios y contratistas del Ministerio de Justicia y del Derecho
FASE II APROPIACIÓN CONCEPTUAL	ARQUITECTURA DE TI	Sensibilización de los conceptos de Arquitectura	Se creara material multimedia con el fin de realizar la sensibilización de los conceptos generales de arquitectura	Mailing-intranet	Pendiente por definir	* Material multimedia * Equipo de uso y apropiación * Funcionarios y
	SEGURIDAD	Sensibilización de los conceptos de Seguridad	Se creara material multimedia con el fin de realizar la sensibilización de los conceptos generales de seguridad	Mailing-intranet	Pendiente por definir	* Material multimedia * Equipo de uso y apropiación * Funcionarios y
	SERVICIOS CIUDADANOS DIGITALES	Sensibilización de los conceptos de Servicios Ciudadanos Digitales	Se creara material multimedia con el fin de realizar la sensibilización de los conceptos generales de Servicios Ciudadanos Inteligentes	Mailing-intranet	Pendiente por definir	* Material multimedia * Equipo de uso y apropiación * Funcionarios y

5.8.1 Presentación de la Estrategia


MISIÓN
El Ministerio de Justicia y del Derecho implementa la política de gobierno digital con el objeto del uso eficiente de Tecnologías de Información y comunicación como base para el desarrollo de sus estrategias organizacionales generando c valor en la prestación de su misión de la entidad.

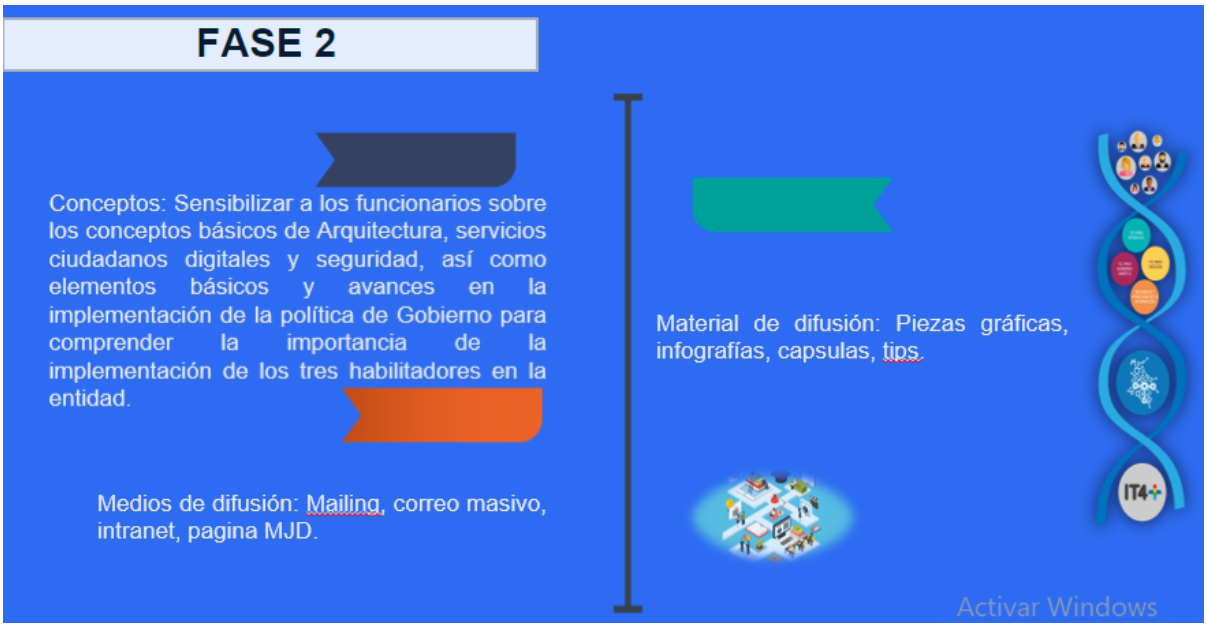

FASES ESTRATEGIA
NIVEL1
FASE DE EXPECTATIVA – ELECCIÓN DE PERSONAJES
FASE APROPIACIÓN CONCEPTUAL
NIVEL 2
NIVEL 3
FASE DIVULGACIÓN NORMATIVIDAD


FASE 1
Pieza expectativa
Emisión de pieza tipo gif anunciando la misión a cumplir invitando a participar de las actividades.
Elección de personajes
Difusión de personajes, elección del personaje de Seguridad, arquitectura y servicios ciudadanos digitales.
Presentación de personajes
Una vez elegidos los personajes, ser realiza difusión de los mismos para conocimiento de loa funcionarios.


PROPUESTA FINAL DE PERSONAJES SEGURIDAD
Misión personaje: Busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.
Cybertron
Segutron


PROPUESTA FINAL PERSONAJES ARQUITECTURA
Misión personaje: Busca fortalecer las capacidades de gestión de T.I. de las entidades públicas, a través de la definición de lineamientos, estándares y mejores prácticas contenidos en el Marco de Referencia de Arquitectura Empresarial del Estado.
Arquitron
Tecnitron
Activar Windows
Ve a Configuración par


PROPUESTA FINAL PERSONAJES SERVICIOS CIUDADANOS DIGITALES
Misión personaje: Busca facilitar y brindar un adecuado acceso a los servicios de la administración pública haciendo uso de medios digitales, para lograr la autenticación electrónica, interoperabilidad y carpeta ciudadana, esto será posible a través de la implementación del Modelo de Servicios Ciudadanos Digitales.
Servitron
Digitron


FASE 2
Conceptos: Sensibilizar a los funcionarios sobre los conceptos básicos de Arquitectura, servicios ciudadanos digitales y seguridad, así como elementos básicos y avances en la implementación de la política de Gobierno para comprender la importancia de la implementación de los tres habilitadores en la entidad.
Medios de difusión: Mailing, correo masivo, intranet, pagina MJD.
Material de difusión: Piezas gráficas, infografías, capsulas, tips.
IT4+
Activar Windows


FASE 3
Apropiación: Se realiza divulgación de normatividad, documentos, guías y demás elementos que deben ser socializados a los funcionarios de la entidad.
Material de difusión: Piezas gráficas, infografías, capsulas, tips.
Medios de difusión: Mailing, correo masivo, intranet, pagina MJD.

A su vez, con la estrategia de uso y apropiación de las TIC, se está llevando a cabo para el personal funcional del Ministerio de Justicia y del Derecho, capacitaciones y formación de TI en:

Capacitaciones

- ✓ Webinar nuevas tendencias tecnológicas
- ✓ Ejercicio de caso de uso de un ataque cibernético
- ✓ Charla de seguridad de la información- Protección de datos personales Ley 1581 de 2012 y 1712 de 2014

Formación en TI

- ✓ CURSO SCRUM FOUNDATIONS incluyendo las 4 certificaciones (Foundation-master.product ower- developer)
- ✓ Curso TOGAF
- ✓ Curso ITIL FOUNDATIONS
- ✓ Curso ISO 20071

Por lo anterior se concluye que, la DTGIJ está cumpliendo con los objetivos para establecer lineamientos que contribuyan a la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información; se recomienda que el plan estratégico cubra en su totalidad los funcionarios y contratistas del MJD, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información.

5.9 Plan de transición de IPv4 a IPv6.

Mediante el MSPI y la guía “G20_Transicion_IPv4_IPv6”, desea proyectar los lineamientos necesarios para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del Estado, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Circular 002 de Julio de 2011, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

Se evidenció que el Ministerio de Justicia y del Derecho (MJD), por medio del contrato 0339-de 2018, realizó la migración del protocolo IPv4 al protocolo IPv6, el cual comprendió:

- ✓ Diagnóstico
- ✓ Planeación
- ✓ Implementación
- ✓ Pruebas de Funcionalidad

A continuación, se detallan las 3 fases de la migración.

Tabla 1 Detalle de la Fase I Planeación

Fase I, Planeación	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Diagnóstico de la Solución	Construcción del Plan de Diagnóstico	7 días	Todo el equipo de Trabajo
	Inventario de TI	2 meses	Ingeniero de Comunicaciones, Gerente de Proyecto
	Análisis de nueva topología de la infraestructura actual y su funcionamiento	3 días	Ingeniero Networking
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos.	20 días	Ingenieros de: Aplicaciones Comunicaciones y Seguridad
	Planeación de migración de los servicios tecnológicos de la entidad.	2 días	Ingeniero Networking
	Validación del estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos.	10 días	Ingeniero de Comunicaciones
	Identificación de esquemas de seguridad de la red de comunicaciones y sistemas de información	5 días	Ingeniero de Seguridad

Tabla 2 Detalle de la Fase II Implementación

Fase II, Implementación	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Desarrollo del Plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.	4 días	Ingeniero de Networking
	Configuración de servicios de DNS, DHCP, Seguridad, VPN y otros	5 días	Ingeniero de Datacenter
	Configuración del protocolo IPv6 en Aplicativos y Sistemas de Comunicaciones	1 mes	Ingeniero de Aplicaciones y Comunicaciones
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	2 semanas	Ingeniero de Seguridad
	Coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6.	1 semana	Gerente de Proyecto

Tabla 3 Detalle de la Fase III Pruebas de Funcionabilidad

Fase III, Pruebas de Funcionalidad	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Pruebas de funcionalidad de IPv6	Pruebas y monitoreo de la funcionalidad de IPv6	2 semanas	Ingeniero de Seguridad
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	2 semanas	Ingeniero de Seguridad
	Afinamiento de las configuraciones de hardware, software, y servicios de MINJUSTICIA.	1 semana	Ingeniero de Comunicaciones

Actualmente la DTGIJ, presenta un monitoreo constante a los equipos de cómputo, servidores y equipos de comunicaciones, verificando que, el último informe periódico al data center, se realizó el 25 de septiembre del presente año; a su vez, se evidencian actividades de chequeo con test de vulnerabilidades, a los diferentes portales del MJD.

5.10 Antecedentes de candidatos a un empleo en el MJD

Se analizan las evidencias entregadas, encontrando que el MJD valida los antecedentes a candidatos a un empleo en el Ministerio de Justicia y del Derecho, a continuación se mencionan los documentos a que se hace alusión en el proceso:

- ✓ **Antecedentes Disciplinarios, fiscales o judiciales**

  La verificación de los antecedentes de los postulados a proveer los empleos vacantes de la planta del Ministerio de Justicia y del Derecho, es validada por el profesional del Grupo de Gestión Humana, con ayuda de los Portales Web o donde las entidades correspondientes dispongan, los antecedentes fiscales, disciplinarios, judiciales y de medidas correctivas del aspirante, dejando las constancias respectivas mediante documento físico impreso.

- ✓ **Manual de Contratación**

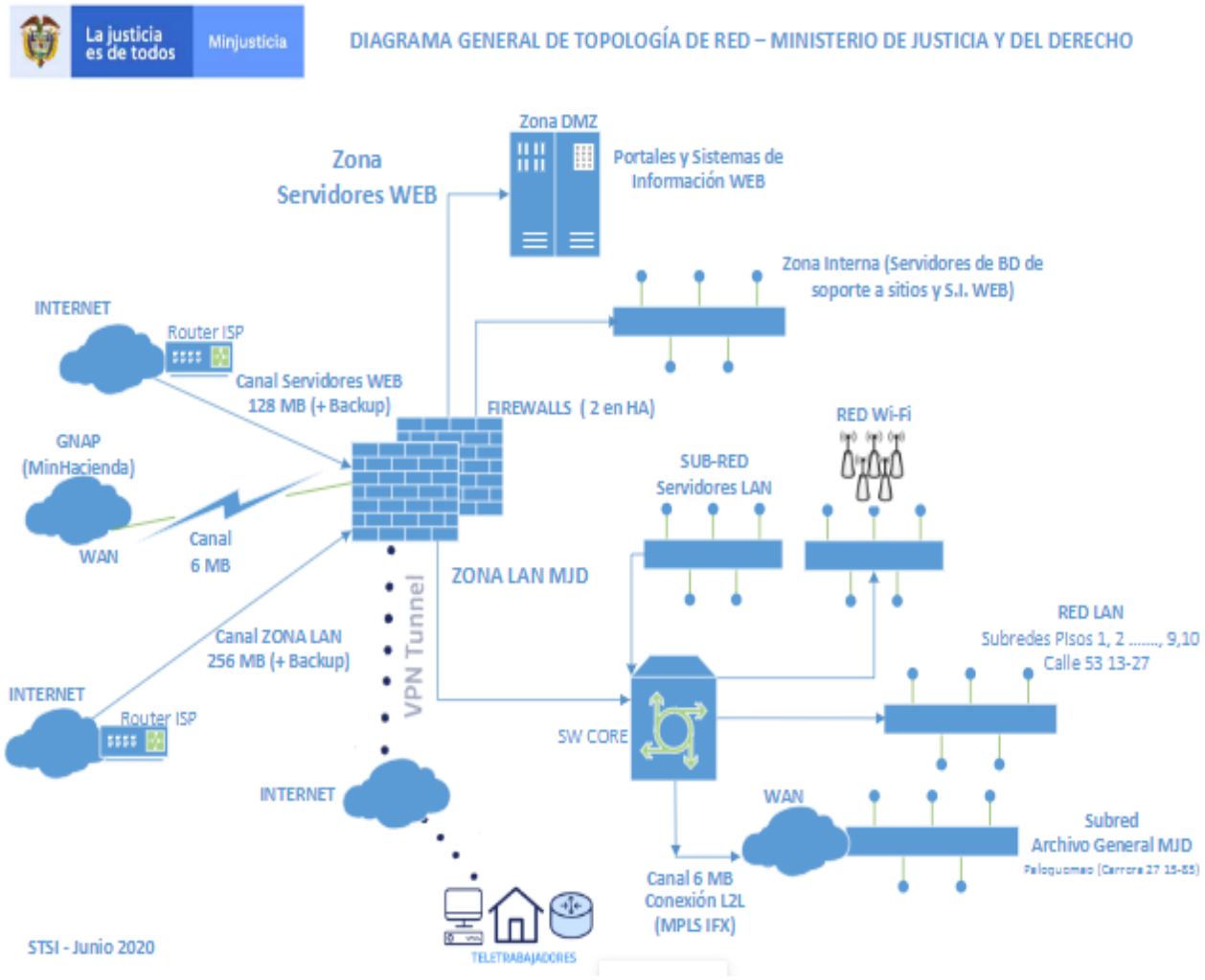
  El manual de contratación se encuentra publicado en el SIG; como responsables están la Secretaría General y Grupo de Gestión Contractual

- ✓ **Ingreso y retiro de Funcionarios**

  Para el ingreso y retiro de funcionarios, se encuentra como responsable del procedimiento el Coordinador(a) de Grupo de Gestión Humana. El procedimiento se encuentra documentado y publicado en el SIG como procedimiento Ingreso y retiro de Funcionarios.

5.11 Diagrama de Red

Se validan las evidencias aportadas, encontrando que la DTGIJ cuenta con una topología de red, en la que se especifican las soluciones de seguridad implementadas en la red.



5.12 Transferencia de Información

La DTGIJ cuenta con un inventario (archivo excel), de las entidades con las cuales el Ministerio de Justicia y del Derecho (MJD), requiere realizar acuerdos de transferencia de información. Para concluir, se identificó -en el inventario- que no hay definido una relación de controles para asegurar la confidencialidad e integridad de la información. Se recomienda robustecer la estructura del inventario, con el fin de proporcionar información más detallada.

La justicia es de todos Minjusticia

Subdirección de Gestión de Información En Justicia

#	Entidades requeridas para Acuerdos de intercambio de información entre el MJD	18/09/2020	25/09/2020
1	Fiscalía General de la Nación -FGN		
2	Instituto Nacional Penitenciario y Carcelario- INPEC		
3	Agencia Nacional de la Defensa Jurídica del Estado- ANDJE	Hoy se insistió con el contacto, para ver si se puede establecer el mecanismo.	pendiente del contacto. informan que eldia martes 29 de septiembre se tendra razón.
4	Unidad de Servicios Penitenciarios y Carcelarios - USPEC	Se recibio respuesta y estan deacuerdo con los documentos (minuta y anexo), Jairo envió los estudios previos el dia de hoy para revisión de parte de la entidad.	Ya la USPEC aprobó la minta, anexo tecnico y estudio previo. se esta a la espera de envio oficial de los documentos con constancia de aprobación para que jairo realice su envio a contractual

5.13 Inventario de Proveedores

El inventario de proveedores que presenta como evidencia la DTGIJ, en su estructura hace referencia al contrato, el objeto y si presenta clausula y acuerdo de confidencialidad.

Se ostentan las siguientes consideraciones que el inventario de proveedores debe tener como:

- La referencia al tipo de activo al que tiene acceso el proveedor
- El periodo de ejecución del contrato
- Si se encuentra en ejecución o si ya fue ejecutado.

Proveedor	Contrato	Objeto	Clausula de Confidencialidad	Acuerdo de Confidencialidad
UT The Factory	0367 de 2020	Prestar los servicios de Fábrica de Software, para los portales y sistemas de información del Ministerio de Justicia y del Derecho	SI	SI
Tiqal S.A.S.	0405 de 2020	Adquirir, implementar y poner en funcionamiento para el Ministerio de Justicia y del Derecho que permita la formulación, integración, seguimiento, publicación y mejora continua a la Planeación Estratégica, el Sistema Integrado de Gestión, el Plan de Acción Institucional y el Plan de Mejoramiento Institucional con sus respectivos indicadores y tableros de control	SI	En trámite
PCT Ltda	0365 de 2019	alquiler) del Sistema de Información PCT-ENTERPRISE a distancia, módulo de Almacén submódulo Control de Bienes muebles para el Ministerio de Justicia y del Derecho	SI	En trámite
Heinsohn Human Global	0369 de 2019	Prestar los servicios de soporte y mantenimiento, mediante la modalidad de bolsa de horas, para el Sistema de Información SIGEP-Gestión Humana del Ministerio de Justicia y del Derecho	SI	En trámite

Se recomienda incluir al inventario de proveedores las consideraciones mencionadas con anterioridad.

5.14 Gestión de Incidentes

La DTGIJ cuenta con el documento “Procedimiento Gestión de Incidentes”, el cual tiene como objetivo “*administrar la seguridad de la información con el fin de proteger la integridad, disponibilidad y confidencialidad de ésta y minimizar el impacto en el negocio de los riesgos y amenazas a los cuales se encuentra expuesta.”*

MINJUSTICIA	PROCEDIMIENTO GESTIÓN DE INCIDENTES	Código: Versión: Vigencia:

1. **PROCESO:** GESTIÓN DE LA INFORMACIÓN Y DE LAS COMUNICACIONES
2. **RESPONSABLE DEL PROCEDIMIENTO:** Subdirección de Tecnologías y Sistemas de Información (en adelante, STSI)
3. **OBJETIVO DEL PROCEDIMIENTO:** Administrar la seguridad de la información con el fin de proteger la integridad, disponibilidad y confidencialidad de ésta y minimizar el impacto en el negocio de los riesgos y amenazas a los cuales se encuentra expuesta. (Objetivo del procedimiento, debe responder el qué, cómo y para qué del procedimiento)
4. **ALCANCE:** Aplica para los contratistas, funcionarios y terceros que gestionen información del Ministerio de Justicia y del Derecho y que puedan afectar su disponibilidad, integridad y/o confidencialidad.

5. DEFINICIONES

Ver el documento Guia 21 - Gestión de Incidentes del modelo de seguridad y privacidad de la información MSPI de MinTIC.

6. POLITICAS DE OPERACIÓN

El documento contiene las políticas de Operación y la gestión de incidentes de seguridad de la Información. Se evidencia que el documento no se encuentra publicado en el SIG, el cual ya fue revisado y aprobado.

RESPONSABILIDAD Y AUTORIDAD		
Elaboró y/o Actualizó:	Revisó:	Aprobó:
Firma:	Firma:	Firma:
Nombre: Martha Liliana Rodríguez Prieto	Nombre: Daniel Iván Montes	Nombre: Reymundo Sojo
Cargo: Contratista	Cargo: Subdirector Tecnologías y Sistemas de Información	Cargo: Director de Tecnologías y Gestión de Información en Justicia

5.15 Plan de Continuidad

Se validaron las evidencias (OneDrive, carpeta #20), en la cual se evidencian dos documentos, uno perteneciente al plan de trabajo y cronograma de actividades, y el segundo, al plan de continuidad con la información consolidada.

Se verifica que el plan de continuidad contiene la Identificación de las aplicaciones y las plataformas consideradas críticas para la operación del MJD.

Sin embargo, se detecta no conformidad, a fin de conocer con precisión los riesgos potenciales de la prestación de servicios de tecnologías de la información en el MJD, es recomendable clasificar los posibles escenarios de los riesgos potenciales y describir su nivel de impacto por cada función crítica del negocio.

Las categorías que aún no se contemplan son:

- ✓ Red Eléctrica
- ✓ Red Datos, Internet y Seguridad
- ✓ Recurso Humano

A su vez, se debe definir -para la metodología del riesgo- la identificación de amenazas y la identificación de vulnerabilidades.

Se identifica una segunda no conformidad, debido que aún no se encuentran contemplados los objetivos que debe contener el plan de continuidad.

A continuación se mencionan los objetivos definidos en la guía N° 20 del MSPI (MinTic).

- ✓ Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones criticas del

negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.

- ✓ Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- ✓ Identificar al personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- ✓ Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- ✓ Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- ✓ Identificar los riesgos presentes para la continuidad.
- ✓ Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- ✓ Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- ✓ Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- ✓ Establecer un plan de prueba, gestión y mantenimiento necesarios para garantizar los objetivos del Plan.

La correcta implementación a la gestión de la continuidad del negocio, disminuirá la posibilidad de ocurrencia de incidentes disruptivos, en caso de producirse, el MJD estará preparado para responder en forma adecuada y oportuna.

6 Análisis de Riesgo:

La información que hace parte del Ministerio de Justicia y del Derecho (MJD) es crucial para su correcto desempeño dentro de la política pública; es por ello que resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un problema para el normal desarrollo de las actividades del MJD.

Dentro del desarrollo de la presente auditoría, y el levantamiento de información, se encontró que la Dirección de Tecnología y Gestión de información en Justicia (DTGIJ), viene adelantando una buena labor con la gestión de riesgos de seguridad de la información con las 26 dependencias de la entidad, basándose en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando identificar y analizar los riesgos del MJD.

A continuación se detallan las actividades realizadas, hasta el momento, por la DTGIJ sobre la Gestión de Riesgos:

- ✓ Establecer el documento "Contexto de Seguridad de la Información DTGIJ".
- ✓ Establecer el documento "Contexto de Seguridad de la Información MJD".
- ✓ Definir los riesgos de seguridad de la información de acuerdo a metodología de gestión de riesgos DAFP.
- ✓ Emitir memorando y planificar reuniones.
- ✓ Establecer herramienta Matriz de Riegos.
- ✓ Sensibilizar las áreas sobre la Metodología de Gestión de Riegos.
- ✓ Gestionar reuniones con cada área indicando el debido diligenciamiento de la matriz de riesgos de seguridad de la información.
- ✓ Realizar reunión de revisión del diligenciamiento para retroalimentar los cambios necesarios en la matriz.
- ✓ Identificar controles para los riesgos que se encuentran en un nivel diferente a bajo.
- ✓ Establecer el plan de tratamiento de riesgos de seguridad de la información.
- ✓ Oficializar el plan de tratamiento de riesgos de seguridad de la información.

6.1 Levantamiento de Riesgos de Seguridad de la Información

Se realiza un análisis a la gestión de riesgos, donde las dependencias realizaron el diligenciamiento de sus activos de información en la herramienta “Riesgos de Seguridad Digital”.

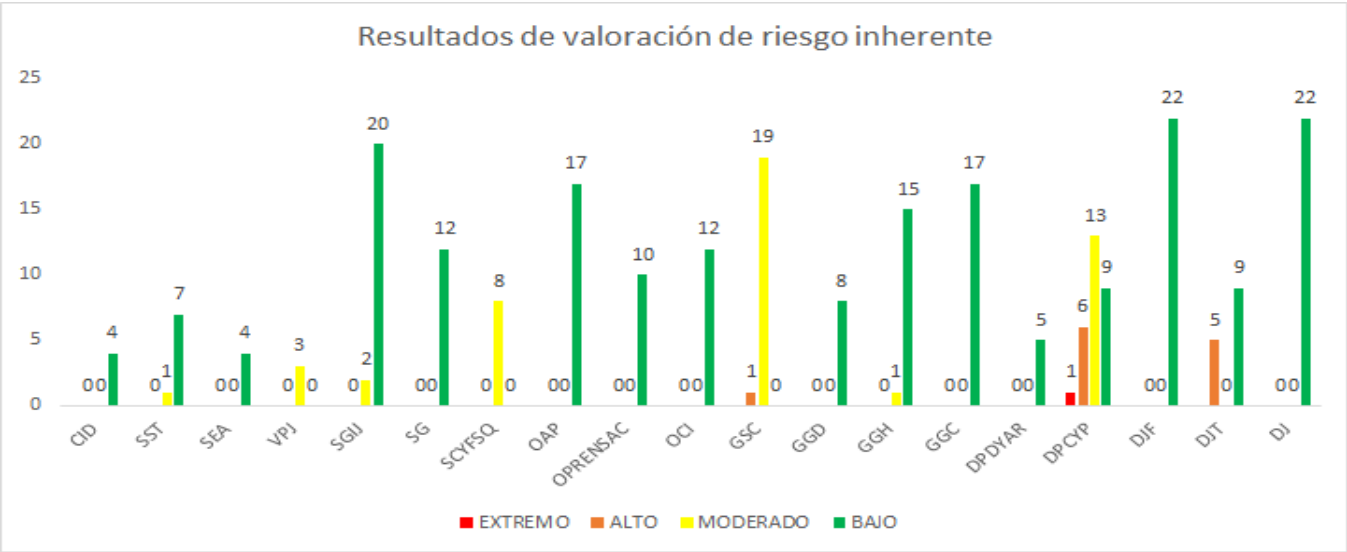
6.1.1 Riesgo Inherente y Residual

Al concluir el diligenciamiento de la herramienta, se observa que de las 26 dependencias del MJD se han diligenciado, revisado y aprobado 19 matrices de riesgos de seguridad de la información las cuales corresponden a:

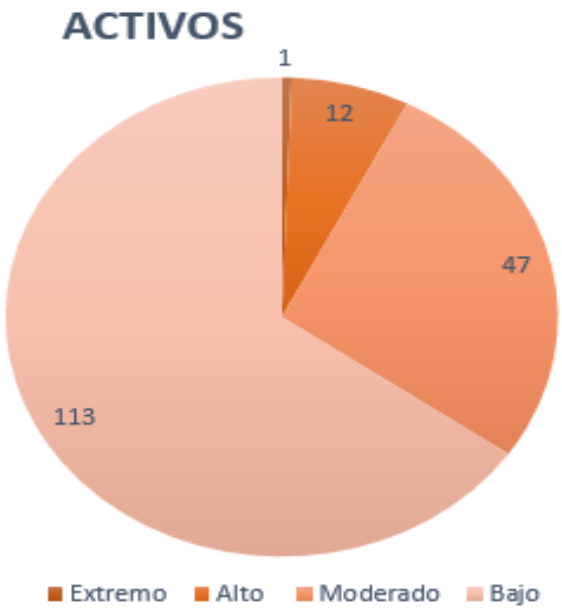
- ✓ CID
- ✓ SST
- ✓ SEA
- ✓ VPJ
- ✓ SGIJ
- ✓ SG
- ✓ SCYFSQ
- ✓ OAP
- ✓ OPRENSAC
- ✓ OCI
- ✓ GSC
- ✓ GGD
- ✓ GGH
- ✓ GGC
- ✓ DPDYAR
- ✓ DPCYP
- ✓ DJF
- ✓ DJT
- ✓ DJ

6.1.1.1 Riesgo inherente

De las 19 dependencias anteriormente mencionadas, la DJ no valoró el riesgo de 20 activos de información; a su vez, la dependencia OPRENSAC no valoró el riesgo de 2 activos de información; por este motivo, no se ven reflejados en la siguiente gráfica.



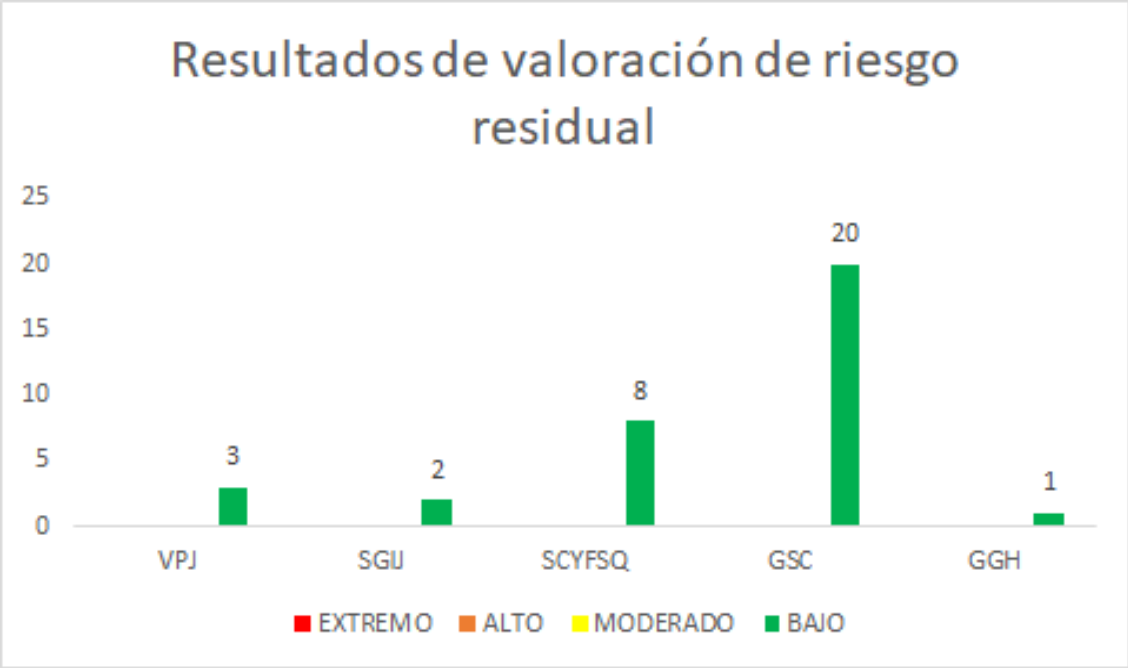
Como se observa en la gráfica anterior “Resultados de valoración de riesgo inherente”, de las 19 dependencias se identificaron los siguientes activos:



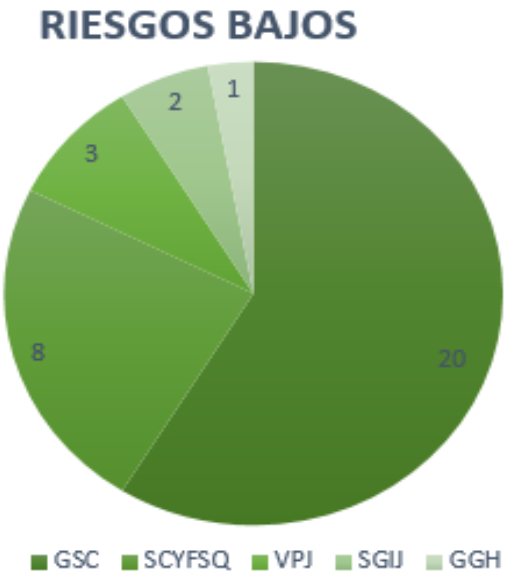
- ✓ 1 activo con una valoración de riesgo extremo.
- ✓ 12 activos con una valoración de riesgo alto
- ✓ 47 activos con una valoración de riesgo moderado
- ✓ 113 activos con una valoración de riesgo bajo

6.1.1.2 Riesgo residual

Para el riesgo residual solo lo presentaron 5 dependencias, con una valoración diferente a bajo, como se puede visualizar en la siguiente gráfica.



Como resultado posterior del establecimiento de controles se identificaron 34 riesgos con valoración baja así:



- ✓ 3 riesgos con una valoración baja en la VPJ
- ✓ 2 riesgos con una valoración baja en la SGIJ
- ✓ 8 riesgos con una valoración baja en la SCYFSQ
- ✓ 20 riesgos con una valoración baja para la GSC
- ✓ 1 riesgo con una valoración baja en el GGH

Concluyendo el análisis de riesgos, la Oficina de Control Interno (OCI) al diligenciar la herramienta "Riesgos de Seguridad Digital", la cual fue liderada por el jefe de la OCI, encontró algunas consideraciones en cuanto a la parametrización de la herramienta, como se menciona a continuación:

"En el trámite del formato no fue posible seleccionar más de una vulnerabilidad (causa) asociada a una amenaza, ni tampoco varias clasificaciones de vulnerabilidad (interna y/o externa) ni las clases de controles (preventivo y/o detectivo) en una misma celda. En este sentido, la parametrización debe permitir la mayoría de causas o vulnerabilidades que generen la amenaza o el riesgo."

Esta consideración fue incluida en el MJD-MEM20-0006193-OCI-1400, adjunto a la respuesta del diligenciamiento de los activos de seguridad de la información de la OCI.

6.2 Seguridad de la información en la gestión de proyectos

Es muy importante que la seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos del Ministerio de Justicia y del Derecho (MJD), para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza.

Para llevar a cabo el análisis de la seguridad de la información en la gestión de proyectos del MJD, se solicitó en el levantamiento de información de la presente auditoría, una descripción de cómo se está implementando en los diferentes proyectos la seguridad de la información.

Se analizan las evidencias aportadas por el auditado (OneDrive carpeta #14), concluyendo no conformidad, ya que estas no soportan la validez de un procedimiento de seguridad de la información en la gestión de proyectos, en la cual no se evidencia integración con en el ciclo de vida de los proyectos, para

asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.

A su vez, se debe tener en cuenta que esto no solamente aplica para proyectos de TI, v. gr puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, contratistas y terceros que soportan procesos del MJD.

7. Conclusiones, hallazgos y/ recomendaciones

7.1 Conclusiones

Es de destacar los trabajos y actividades realizados por la Dirección de Tecnología Gestión e Información en Justicia (DTGIJ) y su Subdirección de Gestión de Información en justicia (SGIJ), la cual viene adelantando un buen trabajo en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), para lo cual se concluye lo siguiente:

- ✓ El MJD cuenta con la política de seguridad de la información, la cual se encuentra aprobada y publicada en el SIG. Se evidenció que la última fecha de emisión de la política es el 6 de Agosto del 2018; desde esta última, no se ha realizado ninguna actualización.

- ✓ La DTGIJ cuenta con el documento “POLITICA DE TECNOLOGIAS DE LA INFORMACIÓN” en cual define directrices y lineamientos sobre el uso y aprovechamiento de las tecnologías de la información implementadas en el Ministerio de Justicia y del Derecho; a su vez, se definen políticas de TI; para esta última, se recomendó incluir las que menciona la guía N° 2 “*Elaboración de la política general de seguridad y privacidad de la información.”* del MSPI (MinTic).

- ✓ Se identificó que en el documento de la política de seguridad de la información, numeral 4.5 “roles y responsabilidades de seguridad de la información”, se evidenciaron no conformidades, las cuales fueron puntualizadas en el desarrollo del presente informe.

- ✓ La DTGIJ viene adelantando el documento “Régimen Sancionatorio”, por el cual, el MJD tenga presente las sanciones por el uso indebido de los activos de información. Este documento aún no se encuentra aprobado, cabe resaltar, que el documento abarca de manera completa las sanciones al uso indebido de los activos de información del MJD.

- ✓ En los activos de Información se concluye que, del 100% del inventario de activos de información, el cual se encuentra en actualización, se tiene un avance del 92%. A su vez, de manera relevante el inventario define el propietario del activo, custodio del activo, se valora el activo de información bajo el criterio de la Ley 1581 2012, tipo de clasificación y por último el respaldo de información.

- ✓ Para los proyectos del MJD, no se evidencia la integración de la Seguridad de la Información, con en el ciclo de vida de los proyectos, lo que asegura que los riesgos de seguridad de la información no se identifiquen y traten como parte del proyecto.

- ✓ La DTGIJ para el plan de comunicaciones, viene adelantando una buena labor con su estrategia “PLAN SENSIBILIZACIÓN USO Y APROPIACIÓN”, para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del MJD.

6.2 Hallazgos

Hallazgo 1

Los roles y responsabilidades para la seguridad de la información contemplada en el documento “Política de Seguridad de la Información”, son insuficientes para abarcar los diferentes niveles (Procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión al cumplimiento de los objetivos del MJD, lo cual presuntamente incumpliría la norma NTC-ISO-IEC 27001-A.6.1.1 “Roles y responsabilidades para la seguridad de la información”, predicable a la luz de lo dispuesto en los criterios establecidos en el Modelo Estándar de Control Interno a la altura del numeral 10.3.

Recomendación

Se recomienda contemplar los roles y responsabilidades de los proveedores y la asignación de personal con las competencias requeridas, contemplados en los lineamientos de la Guía N° 4 “Roles y Responsabilidades” del Modelo de Seguridad y Privacidad de la Información del MinTic.

Hallazgo 2

La Seguridad de la información en la gestión de proyectos no se integra en el ciclo de vida de los proyectos del MJD, ocasionando que los riesgos de Seguridad de la Información no se identifiquen y se puedan tratar como parte del proyecto, lo cual

presuntamente incumpliría la norma NTC-ISO-IEC 27001-A.6.1.5 “Seguridad de la información en la gestión de proyectos”, predicable a la luz de lo dispuesto en los criterios establecidos en el modelo estándar de control interno a la altura del numeral 10.3.

Recomendación

Es necesario involucrar en la operación de la entidad, a cada uno de los procesos y proyectos, el concepto de seguridad de la información, identificando las amenazas que podrían impedir la preservación de la confidencialidad, integridad y disponibilidad de la información en cada caso.

Hallazgo 3

El plan de continuidad que se tiene hasta el momento, carece de posibles escenarios asociados a los riesgos potenciales, los cuales a su turno describan su nivel de impacto por cada función crítica del MJD; a su vez, se debe definir para la metodología del riesgo la identificación de amenazas y la identificación de vulnerabilidades, lo cual presuntamente incumpliría la norma NTC-ISO-IEC 27001-A.17.1.2 “Implementación de la continuidad de la seguridad de la información”, predicable a la luz de lo dispuesto en los criterios establecidos en el modelo estándar de control interno a la altura del numeral 10.3.

Recomendación

Se recomienda robustecer el DRP el cual abarque todos los escenarios de los riesgos potenciales, siguiendo los lineamientos de la guía N° 10 “Continuidad del Negocio” del Modelo de Seguridad y Privacidad de la Información del MinTic.

6.3 Recomendaciones Generales

- Se recomienda para las políticas de Seguridad y Privacidad de la Información, contempladas en el documento “Política de Seguridad de la Información”, incluir las que menciona la guía N° 2 “Elaboración de la política general de seguridad y privacidad de la información.” del MSPI (MinTic).

- Se recomienda para la transferencia de Información robustecer la estructura del inventario, con el fin de proporcionar información más detallada, mencionada en el numeral 5.14.

- Se recomienda para el inventario a proveedores incluir las consideraciones que se mencionaron en el numeral 5.15 del presente informe.

- Se recomienda finalizar lo más pronto el documento “Régimen Sancionatorio”, el cual sea aprobado y publicado en el SIG.

- Se recomienda para las buenas prácticas, establecer contactos de interés con stakeholders que no sean del estado.

- Se recomienda incluir al inventario de proveedores las consideraciones mencionadas con anterioridad en el punto 5.14.

WILMAN FERNANDO MORENO YANQUÉN — Profesional OCI

DIEGO ORLANDO BUSTOS FORERO — Jefe Oficina de Control Interno