PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTIÒN TECNOLOGICA

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

TABLA DE CONTENIDO

pág.

OBJETIVO 4
ALCANCE 5
GLOSARIO 6
PLAN DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL 9
1.1 GENERALIDADES DE LA EMPRESA 9
1.1.1 Necesidades y expectativas de las partes interesadas. 13
1.1.2 Alcance del MSPI. 15
1.1.3 Liderazgo y compromiso de la alta dirección. 16
1.1.4 Roles y responsabilidades. 17
1.1.5 Gestión del riesgo. 20
1.1.5.1 Identificación y valoración de los activos de información. 21
1.1.5.2 Identificación del riesgo. 31
1.1.5.3 Valoración del riesgo. 35
1.1.5.4 Controles asociados a la seguridad de la información. 43

LISTA DE CUADROS

pág.

Cuadro 7. Listado de activos de información IBAL 22
Cuadro 8. Propietario de los activos de información IBAL 24
Cuadro 9. Tipo de activos según MGRSD 25
Cuadro 10. Clasificación de los activos según el tipo 25
Cuadro 11. Clasificación de la información 26
Cuadro 12. Clasificación de los activos según el tipo de información 26
Cuadro 13. Criticidad del activo con respecto a la integridad 27
Cuadro 14. Criticidad del activo con respecto a la disponibilidad 27
Cuadro 15. Criticidad del activo con respecto a la confidencialidad 28
Cuadro 16. Nivel de criticidad con relación a la clasificación 28
Cuadro 17. Clasificación y nivel de criticidad de los activos 29
Cuadro 18. Amenazas identificadas 32
Cuadro 19. Vulnerabilidades identificadas 33
Cuadro 20. Riesgos asociados a la seguridad digital IBAL 34
Cuadro 21. Probabilidad de ocurrencia del riesgo 35
Cuadro 22. Actividades relacionadas con el activo 36
Cuadro 23 Niveles de medición del Impacto del riesgo 38
Cuadro 24. Nivel de impacto en caso de materializarse el riesgo 39
Cuadro 25. Matriz de Calor Inherente 40
Cuadro 26. Zona de riesgo inherente 41
Cuadro 27. Zona de riesgo inherente extremo para la selección de controles 44
Cuadro 28. Controles a implementar en la zona de riesgo inherente extremo 45

OBJETIVO

Analizar los Activos de Información y Recursos del Proceso de Gestión Tecnológica, mediante la aplicación de la Guía de Riesgos del DAFP, para su Valoración, Clasificación y Tratamiento, con el fin de Gestionar la Confidencialidad, Disponibilidad e Integridad de la Información.

ALCANCE

Gestionar los riesgos de seguridad digital asociados a los activos de información, Bases de Datos, Redes y comunicaciones y Servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las actividades de los diferentes procesos de la Empresa.

GLOSARIO

ACTIVO: cualquier cosa que tiene valor para la organización[1].

ACTIVOS DE INFORMACIÓN Y RECURSOS: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo[2].

AMENAZAS: evento que puede generar daño a la información, generada por una vulnerabilidad que puede ser explotada.

CONFIDENCIALIDAD: característica en la seguridad de la información, que limita el acceso a la información a personas no autorizadas.

CONTROL: conjunto de técnicas utilizadas en la seguridad informática, para proteger la información y mitigar los riesgos.

DISPONIBILIDAD: característica de la información que determina que solamente estará accesible a personas autorizadas.

---

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. [Sitio web]. Bogotá: ICONTEC, Norma Técnica NTC-ISO/IEC colombiana 27001. [Consulta: 2021-05-30]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[2] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. [Sitio web]. Bogotá: CONPES, 3854 de 2016. [Consulta: 2021-05-30]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

EVALUACIÓN DEL RIESGO: proceso mediante el cual se identifican los activos, las vulnerabilidades y amenazas, igualmente su probabilidad e impacto, con el fin de identificar los controles a implementar, para mitigar el riesgo.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia de una novedad que comprometa la seguridad informática o la seguridad de la información.

GESTIÓN DEL RIESGO: actividades coordinadas para garantizar la integridad, confidencialidad y disponibilidad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: un evento o serie de eventos que comprometen la seguridad de la información.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos[3].

PLAN DE CONTINUIDAD: documento que brinda una guía de pasos a seguir para continuar operando posterior a un evento o incidente de seguridad de la información.

PARTES INTERESADAS (*STAKEHOLDER*): persona u organización que puede percibirse a sí misma como afectada por una decisión o actividad[4].

RIESGO: probabilidad de materialización de una amenaza.

---

[3] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME. [Consulta: 2021-04-30]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

[4] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Modelo de Seguridad y privacidad de la Información. [Consulta: 2021-04-30]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad[5].

SEGURIDAD DIGITAL: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales[6].

VULNERABILIDAD: debilidad que puede ser explotada por una o varias amenazas.

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Sitio web]. Bogotá: ISO/IEC, NTC-ISO/IEC 17799:2006. [Consulta: 2021-04-30]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[6] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Modelo de Seguridad y Privacidad de la Información. [Consulta: 2021-05-30]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

PLAN DE GESTION DE RIESGOS DE SEGURIDAD DIGITAL

1.1 GENERALIDADES DE LA EMPRESA

El IBAL es una empresa de servicios públicos, que presta los servicios domiciliarios de acueducto y alcantarillado en la ciudad de Ibagué, actualmente tiene las siguientes sedes en la ciudad:

- Sede principal en la K 3 1 04 Barrio La Pola, en esta sede funciona la sede administrativa de la empresa, en ella se encuentran entre otros, el proceso de gestión tecnológica, el datacenter donde se ubican los servidores de la empresa, se tienen centralizadas las comunicaciones (internet de 50 Mbps y canales de datos) y se gestiona toda la seguridad perimetral de la red local y las otras sedes de la empresa.

- Sede la 15. En esta sede localizada en la calle 15 6 48, se encuentran la oficina de los subprocesos de Gestión de Cartera y una parte del proceso de Gestión Atención al cliente y PQR.

- Sede Chapeton. En esta sede localizada en la Vía Chapeton, se encuentra la oficina del proceso de Gestión Documental.

- Sede Calle 60. En esta sede localizada en la calle 60 con 5, se encuentra la oficina del subproceso de facturación y recaudo.

- Sede F25. En esta sede localizada en 5 # 41-16 edificio F25, se encuentra la oficina del subproceso de Gestión Atención al cliente y PQR.

Con relación al aspecto técnico, la empresa tiene una topología de red en estrella en donde hay un datacenter principal y las estaciones de trabajo de todas las sedes,

se conectan a él por medio de canales de datos, los cuales están contratados con la empresa de comunicaciones de Bogotá (ETB). Se tiene una conexión a internet de 50 Mbps (reúso 1:1) contratado con la empresa Media Commerce, la cual es distribuida a las sedes por los canales de datos. Los computadores de la empresa se tienen en una red de dominio de Windows Server, lo que permite administrarlos eficientemente mediante una serie de directivas de grupo las cuales se encuentran en el servidor de dominio y son propagadas por todas las sedes de la empresa, por los canales de datos.

Con relación al aspecto administrativo y organizacional, la empresa tiene un sistema integrado de gestión (SIG), que de acuerdo con el mapa de procesos vigente (ver ilustación 5), se observan los siguientes procesos misionales: Producción de agua potable, Aseguramiento y calidad de agua, Saneamiento Básico, Gestión comercial y Gestión Ambiental.

Profundizando en los procesos misionales del IBAL encontramos que:

- El proceso de producción de agua potable, hace referencia a las actividades que desarrolla el IBAL para captar, transportar, tratar, conducir, almacenar y distribuir el agua potable a los suscriptores de la empresa[7].

- El proceso de aseguramiento de la calidad de agua, hace referencia al monitoreo de la calidad del agua antes, durante y después de su tratamiento, mediante el análisis de las condiciones físico químicas, organolépticas y bacteriológicas[8].

[7] SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS. [sitio web]. Bogotá D.C. SSPD. Sistema único de información Sui. [Consultado: 18 de mayo de 2021]. Disponible en: http://www.sui.gov.co/web/acueducto

[8] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué. IBAL. Laboratorio de control de calidad. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/laboratorio-de-control-de-calidad-luis-eduardo-de-le-n-caicedo

Ilustración 1. Mapa de procesos IBAL

Fuente: EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, sitio web. Disponible en: https://www.ibal.gov.co/sistema-de-gestion-de-calidad

- El proceso de Saneamiento básico, hace referencia a las actividades que desarrolla el IBAL para la recolección de residuos líquidos, la conducción de residuos líquidos, el tratamiento de residuos líquidos y su disposición final[9].

- El proceso de gestión comercial, hace referencia a las actividades para liquidar la factura de los servicios de acueducto y alcantarillado a los suscriptores de la empresa, este proceso se inicia con la lectura de los consumos que se han registrado el micromedidor de agua hasta el recaudo de los servicios prestados. Este conjunto de actividades se realizan de manera mensual y se realizan a la

[9] SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS [sitio web]. Bogotá: SSPD, Sistema único de información Sui. [Consulta: 18 de mayo de 2021]. Disponible en: http://www.sui.gov.co/web/alcantarillado

totalidad de los suscriptores de la empresa, que para agosto de 2021 están en 158,706[10].

- El proceso de gestión ambiental, hace referencia a las actividades para la conservación ambiental, haciendo uso racional y sostenible de los recursos, con el fin de mitigar los aspectos e impactos ambiental que puedan surgir por la prestación de los servicios de acueducto y alcantarillado[11].

Si bien es cierto cada uno de los procesos misionales que tiene EL IBAL son importantes para su operación, se puede observar el proceso de gestión comercial tienen un alto contenido de datos e información, la cual debe gestionarse de manera ágil, oportuna y confiable, ya que, a través de la liquidación de la factura mensual y el recaudo de la misma, la empresa percibe los ingresos necesarios para realizar las inversiones en las redes de acueducto y alcantarillado y así garantizar la prestación de sus servicios.

Se puede concluir que, el conjunto de actividades que se realizan mensualmente en cada uno de los procesos de la empresa IBAL, deben estar coordinadas de principio a fin, y tener un buen apoyo tecnológico que permita agilizar las actividades y garantice la integridad de la información en cada una de ellas, ya que, a través de este, la empresa percibe los recursos necesarios para el cumplimiento del objeto social y un problema en el flujo de actividades del proceso, generaría graves consecuencias económicas para el IBAL.

---

[10] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL. Información de suscriptores facturados servicio de acueducto, periodo de agosto 2021 en SOLIN CLOUD ERP.

[11] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Sistema de gestión ambiental. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/pol-tica-del-sistema-de-gesti-n-ambiental

Por otra parte, continuando con el contexto de los procesos que tiene el IBAL en el SIG, es importante mencionar que a través del proceso de Gestión Tecnológica se tiene que "*Garantizar el efectivo apoyo tecnológico a las diferentes áreas del IBAL S.A. ESP OFICIAL, mediante la asignación, administración y mejora de los recursos tecnológicos disponibles (hardware, software, redes y comunicaciones)*" [12]. Este enfoque que se presenta en la matriz de caracterización del proceso de gestión tecnológica, indica qué a través de este, se deben brindar todas las condiciones técnicas y tecnológicas, para que el cada uno de los funcionarios del IBAL, tenga a su disposición, todas las plataformas informáticas que tiene la entidad con el fin de desarrollar las actividades diarias, en función de los procesos a que pertenecen.

1.1.1 Necesidades y expectativas de las partes interesadas. Con el fin de identificar las partes interesadas para el desarrollo de este proyecto, a continuación, se hace una relación de cargos que pueden verse afectados en caso que ocurra un incidente relacionado con la seguridad de la información.

- **Gerente**. Encargado desarrollar los procesos de planeación, organización, control, orientación, ejecución y dirección, así como ejecutar las disposiciones de la asamblea general, y la junta directiva[13]. Deberá ser el responsable de velar por la implementación de las políticas relacionadas con la seguridad y privacidad de la información, en el marco del cumplimiento de su función legales establecidas en la resolución IBAL 0755 de 03 de agosto de 2018.

---

[12] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Matriz de caracterización gestión tecnológica. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20TECNOLOGICA%20v14.pdf

[13] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

- **Dirección comercial y de servicio al cliente**. Responsable de la planeación, ejecución y control de las políticas, planes, programas y proyectos comerciales, mediante una adecuada y oportuna gestión comercial14. Deberá velar por la planeación y ejecución de las actividades del proceso de gestión comercial, con el fin de garantizar el correcto tránsito de información entre actividades que conforman el proceso.

- **Líder del proceso de facturación y recaudo.** Responsable de planear, coordina y controlar la ejecución del proceso de facturación, el cual incluye las actividades de cargue de información, lectura, crítica, post-crítica, visitas de desviación, liquidación, impresión y entrega de facturas15. Con relación a las necesidades y expectativas el líder del proceso de facturación y recaudo, es el responsable de coordinar y velar por la ejecución de todas las actividades del proceso de facturación.

- **Líder del proceso de gestión tecnológica**. Responsable de la administración, control de la infraestructura, seguridad integral de la plataforma tecnológica y los sistemas de información del IBAL, contribuyendo a garantizar la protección, confidencialidad, integridad y disponibilidad de la información y los sistemas de información[16]. Con relación a las necesidades y expectativas el líder del proceso

[14] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

[15] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

[16] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consultado: 18 de mayo de 2021]. Disponible en:

de gestión tecnológica, es el responsable de la garantizar la disponibilidad, integridad, confidencialidad y seguridad de la información en el IBAL.

1.1.2 Alcance del MSPI. Para determinar el alcance del MSPI para el IBAL, es importante conjugar varios factores con el fin de determinar los límites y la aplicabilidad que se le dará al modelo en la fase de implementación.

- Como primer factor se tiene que, el proceso de gestión tecnológica es, por su alta complejidad, altos volúmenes de información e importancia para la operación de la empresa, el proceso sobre el cual se va a centrar la planificación del modelo.

- Como segundo factor se tiene que el proceso de gestión tecnológica, será el responsable de realizar la gestión de los riesgos asociados a la seguridad de la información de cada uno de los procesos de la empresa, así como el de diseñar e implementar los controles necesarios con el fin de eliminar las vulnerabilidades que se puedan detectar en los elementos que conforman los sistemas de información de este proceso, con el fin de reducir el impacto que puede generar un incidente de seguridad. Así mismo deberá elaborar y auditar periódicamente los planes de contingencia y de recuperación ante posibles fallas o incidentes, que comprometan de la información corporativa.

- Como tercer factor que se debe tener en cuenta para la planificación del modelo, es el resultado de diagnóstico que se obtuvo a través del diligenciamiento del Instrumento de Evaluación MSPI, el cual permite determinar el estado actual de la gestión de seguridad y privacidad de la información en el IBAL y las

https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

vulnerabilidades administrativas y técnicas con relación a los dominios del anexo A de la norma ISO/IEC 27001:2013. Los resultados que se van a reforzar durante la planificación son los que resultaron INEXISTENTE, INICIAL Y REPETIBLE según la evaluación de efectividad de control, los cuales son:

- A.5 Políticas de seguridad de la información.
- A.8 Gestión de activos.
- A.10 Criptografía.
- A.15 Relaciones con los proveedores.
- A.16 Gestión de incidentes de seguridad de la información.
- A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.

1.1.3 Liderazgo y compromiso de la alta dirección. El IBAL su sistema integrado de gestión, tiene delegado por acto administrativo a un funcionario encargado de liderar las actividades encaminadas a la gestión de los sistemas certificados por la empresa (OHSAS 18001, ISO 14001 e ISO 9001:2015), por ende, a este funcionario se le deberán las responsabilidades asociadas al MSPI, como parte de sus funciones.

Así mismo acorde con lo dispuesto en el Decreto 1499 de 2017[17] "*…Decreto Único Reglamentario del Sector Función Pública..*" en cada una de las entidades públicas del estado, deberá existir un **Comité Institucional de Gestión y Desempeño,** el cual atenderá todos los temas relacionados con la implementación y desarrollo de

[17] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Decreto 1499 (11, septiembre, 2017). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433

las políticas de gestión de la empresa, motivo por el cual es importante definir que, a través de este comité, se realizarán todas las gestiones encaminadas a implementar, operar, evaluar y garantizar el mejoramiento continuo del modelo a través de las siguientes funciones:

- Coordinar la inclusión en el manual especifico de funciones y competencias laborales de la empresa, funciones relacionadas con seguridad y privacidad de la información, así como los funcionarios a los que se les delegará esta responsabilidad.

- Planear y coordinar las estrategias relacionadas con la publicación y adopción de la política general del modelo, los objetivos y las políticas específicas de seguridad y privacidad de la información.

- Planear y coordinar los recursos necesarios para la implementación, seguimiento y mejoramiento continuo del MSPI.

- Realizar las revisiones periódicas al MSPI, con el fin de planear las posibles acciones de mejora o acciones correctivas, que garanticen la continuidad del modelo.

- Entre otras que resulten de la planificación e implementación del MSPI.

1.1.4 Roles y responsabilidades. Para el desarrollo del MSPI es importante definir los roles y responsabilidades para garantizar el cumplimiento de los objetivos del modelo.

- **Gerencia.**

- Adoptar la política de seguridad y privacidad de la información, sus objetivos y políticas específicas.

- Garantizar la disponibilidad de recursos financieros, humanos, técnicos y tecnológicos que se requieran para implementar la política de seguridad y privacidad de la información.

- Comunicar a la empresa la importancia del MSPI.

- Asegurar que el MSPI logre los resultados previstos.

- Realizar las revisiones periódicas a la adopción del MSPI.

▪ **Proceso de Gestión Tecnológica.**

- Apoyar las actividades relacionadas con el autodiagnóstico, planificación, operación, evaluación y mejoramiento continuo del MSPI.

- Realizar la difusión y socialización de la presente política de seguridad y privacidad de la información.

- Elaborar y actualizar la documentación de todos los procedimientos, protocolos, instructivos, guías y manuales, que se deriven de la presente política de seguridad y privacidad de la información.

- Garantizar la adopción y realizar seguimiento de los controles relacionados en la política de seguridad y privacidad de la información del IBAL.

- Gestionar de una manera adecuada, el inventario de activos de información y recursos tecnológicos de propiedad o bajo custodia del IBAL, relacionados en el MSPI.

- **Proceso de Gestión Humana.**

- Garantizar qué se incluya en el programa de capacitaciones planeadas por la empresa, la política de seguridad y privacidad de la información y los cambios que en ella se realicen.

- Gestionar la inclusión de los artículos necesarios en el manual especifico de funciones y competencias laborales de la empresa, relacionados con las actividades desarrolladas en el MPSI.

- **Proceso de Gestión Jurídica y Contractual**

- Gestionar la inclusión en las minutas de los contratos suscritos entre el IBAL y terceros, acuerdos de confidencialidad relacionadas con los activos de información que tengan acceso por el desarrollo del objeto contractual.

- **Control Interno de Gestión.**

- Incluir en el plan anual de auditorías, mecanismos de verificación para evaluar e informar sobre el cumplimiento de la implementación de la política de seguridad y privacidad de la información.

- Elaborar informes para la gerencia sobre el cumplimiento de la política de seguridad y privacidad de la información.

- Realizar las recomendaciones necesarias para el cumplimiento de la política de seguridad y privacidad de la información.

Funcionarios, contratistas y demás partes interesadas.

- Deberán conocer y cumplir a cabalidad la política de seguridad y privacidad de la información y los requisitos que ella impone, so pena las sanciones disciplinarias que acarreé el incumplimiento de la misma.

- Participar activamente en las capacitaciones relacionadas con la política de seguridad y privacidad de la información.

1.1.5 Gestión del riesgo. Una vez identificado los factores más relevantes para la fase de planificación, se procede a detallar la metodología realizar la gestión del riesgo en los activos de información. Para esto se tomará como base la *GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS DEL DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (EN ADELANTE DAFP)* Versión 5 de diciembre de 2020[18].

De acuerdo con la guía del DAFP, se tiene que realizar los siguientes pasos para la gestión del riesgo:

[18] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Guía para la administración del riesgo y el diseño de controles en entidades pública. Versión 5 diciembre de 2020. [Consulta: 18 de mayo de 2021]. Disponible en: 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?t=1611247032238&download=true

1.1.5.1 Identificación y valoración de los activos de información. Inicialmente, es importante conocer que un activo es cualquier componente que juega un papel importante dentro de los procesos que se realizan en el grupo de gestión Tecnológica, por ejemplo: aplicaciones, servicios web, redes de comunicaciones, datos físicos o digitales, bases de datos, dispositivos, entre otros. Es por ello, que se hace relevante identificar y determinar cuáles son los elementos que se deben de proteger y con esto garantizar que la prestación de los servicios dentro del IBAL se realice dentro de un entorno digital seguro.

Para realizar la adecuada gestión de los activos de seguridad de la información en el IBAL, deberán realizarse las siguientes preguntas:

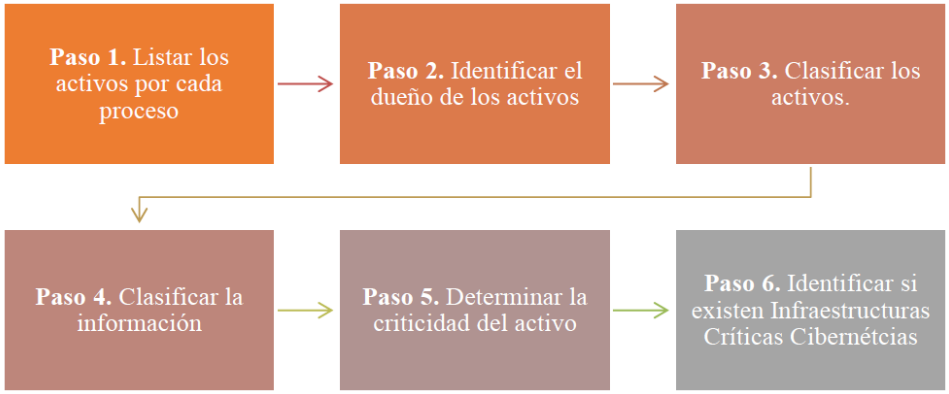
¿Qué activos son esenciales para que el proceso de gestión tecnológica cumpla con los objetivos plasmados en él SIG?

¿Cuáles son los activos esenciales para el desarrollo de las actividades de cada uno de los procesos con los que cuenta el IBAL?

Una vez planteados estos dos interrogantes, es importante desarrollar los pasos que se mencionan en el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas en adelante ***MGRSD***[19]. De acuerdo con el MGRSD, se deben realizar los siguientes pasos para la identificación y valoración de activos, como se muestra en la ilustración 6.

[19] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. [Consulta: 18 de mayo de 2021]. Disponible en: 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

Ilustración 2. Pasos para la identificación y valoración de activos



Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS, Versión 1. Página 12.

A continuación, se detallan cada uno de los pasos:

- **Paso 1. Listar los activos para cada proceso**. Dentro de los procesos de Gestión Tecnológica del IBAL, se identificaron y se listaron los activos señalando el identificador único, nombre del activo, su respectiva descripción y el proceso al que pertenece. El listado que se puede consultar en el cuadro 7.

Cuadro 1. Listado de activos de información IBAL

ID Activo	Proceso	Nombre del Activo	Descripción del Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Permiten capturar los datos de las lecturas mensualmente de los micromedidores de agua de los suscriptores del IBAL.
GC-002	Gestión Comercial	Catastro de suscriptores	Datos de los suscriptores de la empresa a los cuales se les presta el servicio de acueducto y alcantarillado. Con estos datos, los consumos y tarifas, se realiza proceso de liquidación de la factura.
GC-003	Gestión Comercial	Recurso Humano	Funcionarios administrativos y operarios encargados de la toma de lecturas, relecturas, revisiones internas y entrega de facturas, análisis de consumos, liquidación de la factura y gestión de las novedades del proceso comercial (pqr, pagos, abonos, financiaciones, etc).

GC-004	Gestión Comercial	Documentos en papel	Conformado por los documentos en físico necesarios para realizar algunas de las actividades del proceso comercial, entre los cuales están: las notificaciones para revisión interna, las revisiones internas y toma de lecturas manual.
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Software ERP para gestionar la información de todos los procesos del IBAL, responsable de realizar el proceso de liquidación de la factura del servicio a los suscriptores. Software on-premise.
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Base de datos relacional en MS SQL SERVER 2014, con la información de todos los procesos del IBAL, entre ellos el catastro de suscriptores.
GT-003	Gestión Tecnológica	Intranet	Software de aplicación basada en la web, para gestionar los datos de la toma de lecturas a través de los dispositivos celulares. Software on-premise.
GT-004	Gestión Tecnológica	Base de datos Intranet	Base de datos relacional en MS SQL SERVER 2017 EXPRESS, con los datos del proceso de toma de lecturas a través de los dispositivos celulares.
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Compuesto por el hardware y el software de sistema, software de servicios, por medio del cual se ejecuta el software SOLIN ERP.
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Compuesto por el hardware y el software de sistema y software de servicios, por medio del cual se almacenan los datos e información del software SOLIN ERP.
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Compuesto por el hardware y el software de sistema y software de servicios por medio del cual se ejecutan el software de aplicaciones de la intranet.
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Compuesto por el hardware y el software de sistema y software de servicios por medio del cual se almacenan los datos e información de la intranet.
GT-009	Gestión Tecnológica	Canales de Datos	Canales de comunicación de datos entre las sedes de la empresa y la sede principal del IBAL, contratados con ETB, tienen un ancho de banda de 15 Mbps.
GT-010	Gestión Tecnológica	Servicio de Internet	Canal dedicado para la conexión a internet de 50 Mbps, con reúso 1:1, el servicio de internet es gestionado y distribuido a todas las sedes de la empresa desde la sede principal del IBAL.
GT-011	Gestión Tecnológica	Firewall	Sistema de seguridad perimetral, con funciones de control de puertos, IDS, IPS y control de navegación, entre otros.
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Switch capa 2, localizado en el rack de comunicaciones, permite conectar el firewall con los otros dispositivos de comunicación.
GT-013	Gestión Tecnológica	Switch Core Servidores	Switch capa 2, localizado en el rack de servidores, permite la comunicación entre los servidores y el Switch del rack de comunicaciones.
GT-014	Todos	Computadores usuarios finales	Dispositivos de trabajo de los funcionarios de la empresa, por medio del cual acceden al software SOLIN, la intranet e internet para realizar sus actividades diarias.
GT-015	Todos	Antivirus	Sistema de protección contra malware que se instala en los computadores de los usuarios finales y servidores de la empresa.
GT-016	Gestión Tecnológica	Datacenter	Espacio físico para el alojamiento de los servidores y centralización de las comunicaciones del IBAL. En él se encuentran el rack de servidores y el rack de comunicaciones con unas condiciones ambientales y eléctricas controladas para su funcionamiento.

Fuente: elaboración grupo de trabajo.

- **Paso 2. Identificar el dueño de los activos**. En este paso, se debe de reconocer el propietario designado para cada uno de los activos identificados, con el propósito de designar los responsables de la protección y mantenimiento de estos elementos, esta información se puede ver en el cuadro 8.

Cuadro 2. Propietario de los activos de información IBAL

ID Activo	Proceso	Nombre del Activo	Propietario Designado del Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Operarios de facturación
GC-002	Gestión Comercial	Catastro de suscriptores	Líder del proceso de gestión comercial
GC-003	Gestión Comercial	Recurso Humano	Líder del proceso de gestión comercia
GC-004	Gestión Comercial	Documentos en papel	Líder subproceso de Gestión Cartera Líder subproceso de facturación y recaudo Líder subproceso de Gestión de atención al cliente y pqr
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-003	Gestión Tecnológica	Intranet	Líder del proceso de Gestión tecnológica
GT-004	Gestión Tecnológica	Base de datos Intranet	Líder del proceso de Gestión tecnológica
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Líder del proceso de Gestión tecnológica
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Líder del proceso de Gestión tecnológica
GT-009	Gestión Tecnológica	Canales de Datos	Líder del proceso de Gestión tecnológica
GT-010	Gestión Tecnológica	Servicio de Internet	Líder del proceso de Gestión tecnológica
GT-011	Gestión Tecnológica	Firewall	Líder del proceso de Gestión tecnológica
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Líder del proceso de Gestión tecnológica
GT-013	Gestión Tecnológica	Switch Core Servidores	Líder del proceso de Gestión tecnológica
GT-014	Todos	Computadores usuarios finales	Funcionarios del IBAL
GT-015	Todos	Antivirus	Líder del proceso de gestión tecnológica
GT-016	Gestión Tecnológica	Datacenter	Líder del proceso de gestión tecnológica

Fuente: elaboración grupo de trabajo.

- **Paso 3. Clasificar los activos**. Se determinó para cada activo identificado, a que grupo de activos según su naturaleza pertenece. Para realizar esta clasificación se tomó como referencia la tipología de activos que sugiere el MGRSD (Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas), como se muestra en el cuadro 9.

Cuadro 3. Tipo de activos según MGRSD

Tipo de Activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores)
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos,
Intangibles	activos inmateriales que otorgan a la entidad una ventaja competitiva
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red
Personas	Roles que, por su conocimiento, experiencia y criticidad son considerados activos de información
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS. Versión 1. Página 13 y 14.

A continuación, se realiza la clasificación de los activos de información identificados en el IBAL, de acuerdo con la tipología del MGRSD, como se puede ver en el cuadro 10.

Cuadro 4. Clasificación de los activos según el tipo

ID Activo	Proceso	Nombre del Activo	Tipo de Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Hardware
GC-002	Gestión Comercial	Catastro de suscriptores	Información
GC-003	Gestión Comercial	Recurso Humano	Personas
GC-004	Gestión Comercial	Documentos en papel	Información
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Software
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Información
GT-003	Gestión Tecnológica	Intranet	Software
GT-004	Gestión Tecnológica	Base de datos Intranet	Información
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Hardware y software
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Hardware y software
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Hardware y software
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Hardware y software
GT-009	Gestión Tecnológica	Canales de Datos	Componente de red
GT-010	Gestión Tecnológica	Servicio de Internet	Servicios
GT-011	Gestión Tecnológica	Firewall	Hardware
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Componente de red
GT-013	Gestión Tecnológica	Switch Core Servidores	Componente de red
GT-014	Todos	Computadores usuarios finales	Hardware y software
GT-015	Todos	Antivirus	Software
GT-016	Gestión Tecnológica	Datacenter	Instalaciones

Fuente: elaboración grupo de trabajo.

- **Paso 4. Clasificar la información**. Para realizar la clasificación de la información se tomó como directrices las leyes 1712 de 2014 y 1581 de 2012, así como también la guía 5 Gestión de activos del Modelo de Seguridad y Privacidad de la Información, como se muestra en el cuadro 11.

Cuadro 5. Clasificación de la información

Clasificación	Descripción
Información pública	Información de acceso libre para cualquier persona u o entidad que la requiera. / No contiene datos personales.
Información pública clasificada	Información confidencial para la gestión de los procesos de la empresa. Puede ser accedida por terceros con autorización. / Contiene datos personales.
Información pública reservada	Información disponible únicamente para procesos de la empresa. / Contiene datos personales

Fuente: COLOMBIA. Congreso de la República, Ley 1712 de 2014. Página 3. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf

En el cuadro 12, se puede ver la clasificación de los activos según el tipo de información.

Cuadro 6. Clasificación de los activos según el tipo de información

ID Activo	Proceso	Nombre del Activo	Clasificación de los activos según el tipo de información
GC-001	Gestión Comercial	Dispositivos Celulares	Información pública clasificada
GC-002	Gestión Comercial	Catastro de suscriptores	Información pública reservada
GC-003	Gestión Comercial	Recurso Humano	Información pública
GC-004	Gestión Comercial	Documentos en papel	Información pública clasificada
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Información pública clasificada
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Información pública reservada
GT-003	Gestión Tecnológica	Intranet	Información pública clasificada
GT-004	Gestión Tecnológica	Base de datos Intranet	Información pública clasificada
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Información pública reservada
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Información pública reservada
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Información pública reservada
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Información pública reservada
GT-009	Gestión Tecnológica	Canales de Datos	Información pública clasificada
GT-010	Gestión Tecnológica	Servicio de Internet	Información pública
GT-011	Gestión Tecnológica	Firewall	Información pública reservada
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Información pública reservada
GT-013	Gestión Tecnológica	Switch Core Servidores	Información pública reservada
GT-014	Todos	Computadores usuarios finales	Información pública clasificada
GT-015	Todos	Antivirus	Información pública reservada
GT-016	Gestión Tecnológica	Datacenter	Información pública reservada

Fuente: elaboración grupo de trabajo.

- **Paso 5. Determinar la criticidad del activo**. Para realizar la evaluación de la criticidad de los activos, se tuvo en cuenta el grado de importancia de cada uno respecto a la confidencialidad, integridad y disponibilidad, así se logró identificar el nivel de importancia o criticidad para el proceso de gestión tecnológica. Las escalas utilizadas para esta valoración fueron referidas de la Guía 5. Gestión de Activos del MSPI.

  Para la clasificación de los activos de acuerdo con la integridad, se utilizará ALTA MEDIA y BAJA, los activos de información que aún no se puedan clasificar según su integridad, serán tratados como ALTA. Ver cuadro 13.

Cuadro 7. Criticidad del activo con respecto a la integridad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La Información debe ser precisa coherente y completa, su pérdida no genera consecuencias
Información pública clasificada	(M) MEDIA	La Información debe ser precisa coherente y completa, su pérdida genera impacto negativo leve
Información pública reservada	(A) ALTA	La Información debe ser precisa coherente y completa, su pérdida genera graves consecuencias

Fuente: Elaboración del grupo de trabajo

Para la clasificación de los activos de acuerdo con la disponibilidad (por que puede ser consultada o utilizada por una individuo, proceso o entidad), se utilizará ALTA, MEDIA y BAJA, los activos de información que aún no se puedan clasificar según la disponibilidad, serán tratados como ALTA, ver cuadro 14.

Cuadro 8. Criticidad del activo con respecto a la disponibilidad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La no disponibilidad no con lleva implicaciones de ningún índole
Información pública clasificada	(M) MEDIA	La no disponibilidad genera implicaciones índole legal o económico
Información pública reservada	(A) ALTA	La no disponibilidad genera implicaciones índole legal y pérdidas de tipo económico.

Fuente: Elaboración del grupo de trabajo

Para la clasificación de los activos de acuerdo con la confidencialidad (la información no esté disponible ni será revelada a individuos, entidades o procesos no autorizados), se utilizará ALTA, MEDIA y BAJA, los activos de información que aún no se puedan clasificar según la confidencialidad, serán tratados como ALTA Ver cuadro 15.

Cuadro 9. Criticidad del activo con respecto a la confidencialidad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La Información está sin restricción de uso o conocimiento, la pérdida de confidencialidad no genera consecuencias
Información pública clasificada	(M) MEDIA	Información de la entidad y de sus terceros, puede ser accedida con autorización. la pérdida de confidencialidad genera consecuencias leves
Información pública reservada	(A) ALTA	Información de uso exclusivo para la empresa. la pérdida de confidencialidad genera consecuencias graves

Fuente: Elaboración del grupo de trabajo

Teniendo en cuenta que el nivel de criticidad, es el cálculo que determina el valor del activo en relación con la clasificación de la información, se tienen la siguiente escala de en el cuadro 16.

Cuadro 10. Nivel de criticidad con relación a la clasificación

Nivel de Criticidad	Clasificación
BAJA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad, es baja
MEDIA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad, en una de sus propiedades es alta o al menos en una de ella es de nivel medio
ALTA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad es alta.

Fuente: Elaboración del grupo de trabajo

Una vez establecidos los parámetros para evaluar el nivel de criticidad de los activos identificados en el IBAL, se realiza la respectiva clasificación y se determina el nivel de criticidad de cada uno de estos activos, como se puede ver en el cuadro 17.

Cuadro 11. Clasificación y nivel de criticidad de los activos

ID Activo	Nombre del Activo	Integridad	Disponibilidad	Confidencialidad	Nivel de Criticidad
GC-001	Dispositivos Celulares	M	M	M	M
GC-002	Catastro de suscriptores	A	A	A	A
GC-003	Recurso Humano	B	M	B	B
GC-004	Documentos	M	M	M	M
GT-001	Solin CLOUD ERP	A	A	A	A
GT-002	Base de datos SOLIN CLOUD ERP	A	A	A	A
GT-003	Intranet	M	A	M	M
GT-004	Base de datos Intranet	M	A	M	M
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	A	A	A	A
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	A	A	A	A
GT-007	Servidor de Aplicaciones INTRANET	M	A	M	M
GT-008	Servidor de Base de datos INTRANET	M	A	M	M
GT-009	Canales de Datos	M	M	M	M
GT-010	Servicio de Internet	B	M	M	M
GT-011	Firewall	A	A	A	A
GT-012	Switch Core Comunicaciones	A	A	A	A
GT-013	Switch Core Servidores	A	A	A	A
GT-014	Computadores usuarios finales	M	B	A	A
GT-015	Antivirus	A	A	A	A
GT-016	Datacenter	A	A	A	A

Fuente: elaboración grupo de trabajo.

- **Paso 6. Identificar si existen infraestructuras críticas cibernéticas ICC**. Realizados los pasos anteriores, se procedió a determinar si los activos de información que se identificaron son servicios esenciales y si estos están catalogados como Infraestructura Critica Cibernética (ICC), por que superan alguno de los tres criterios de acuerdo con los lineamientos impartidos por la DAFP, en la ilustración 7.

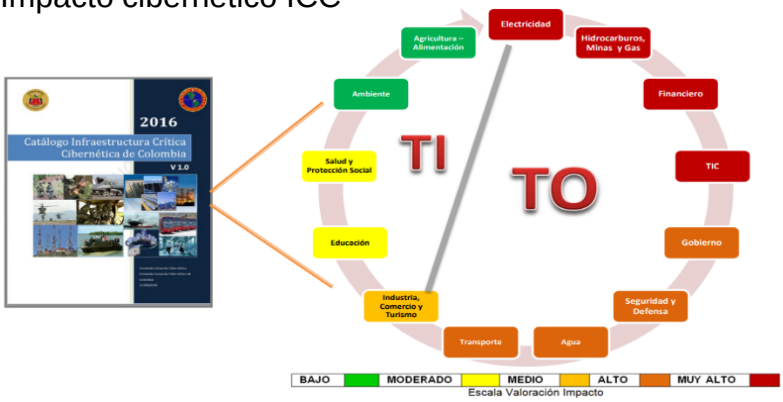
Ilustración 3. Criterios para identificar ICC

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS. Versión 1. Página 18.

Teniendo en cuenta el concepto del Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares de Colombia, sobre infraestructura crítica cibernética "*Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*[20]", se puede concluir ante un eventual incidente o perturbación que afecte alguno de los activos de información que se identificaron en el IBAL, ninguno de ellos tendría un grave impacto para los usuarios y/o suscriptores de la empresa, que supere los criterios para clasificarlos como ICC, porque ninguno de ellos está enfocado a las TO, como se muestra en la ilustración 8.

Ilustración 4. Impacto cibernético ICC



Fuente: Comando Conjunto Cibernético (CCOC) Página 3. Disponible en: https://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticas-ciber-en-colombia.pdf

[20] ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS [sitio web]. Bogotá: ACIS. Conferencia Comando Conjunto Cibernético, fuerzas militares de Colombia. [Consultado: 18 de mayo de 2021]. Disponible en: https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

1.1.5.2 Identificación del riesgo. Una vez realizada la identificación de los activos información, se realiza la definición de los riesgos asociados a los procesos de gestión tecnológica, donde se tomaron para esta identificación todos los activos valorados en la fase anterior.

Según lo indica la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" presentada por el DAFP, se podrán identificar los siguientes tres (3) riesgos asociados a la seguridad digital: ***perdida de confidencialidad, perdida de integridad y perdida de la disponibilidad***.

Para cada uno de los riesgos identificados, se deben relacionar el grupo de activos específicos del proceso y, simultáneamente, identificar las posibles amenazas y vulnerabilidades que podrían ocasionar la materialización de estos. Es por ello, que para realizar la identificación de los riesgos que pueden afectar los activos, se deben evaluar las amenazas y las vulnerabilidades en razón a las perdidas en la confidencialidad, integridad y disponibilidad de la información, de la coexistencia de estas dos, depende el riesgo.

La identificación de riesgos, amenazas y vulnerabilidades, se realizó a través del ***análisis de escenarios***, en la cual se expusieron una serie de situaciones las cuales pueden generar perdida de la confidencialidad, integridad y disponibilidad de la información, en el proceso de gestión tecnológica.

A continuación, en el cuadro 18, se identificaron las siguientes amenazas relacionadas con los objetivos del proceso de gestión tecnológica, los cuales pueden generar daño a los activos por medio de la explotación de las vulnerabilidades.

Cuadro 12. Amenazas identificadas

Amenaza	Descripción
Acceso no autorizado	Hace referencia al acceso indebido a los recursos de software (sistema operativo, aplicaciones, etc) o al centro de datos por falta de controles efectivos que impidan esta situación.
Destrucción de información	Hace referencia a la pérdida parcial o completa de los datos o información.
Fallas en el hardware	Posibles fallos técnicos que se pueden presentar en la infraestructura tecnológica, como servidores, computadores, terminales portátiles, etc.
Fallas en el software	Posibles fallas a nivel de aplicaciones que suscitan que los procesos tecnológicos presenten resultados inesperados, lo que genera retrasos en las actividades y hasta parálisis en los procesos.
Fallas en las comunicaciones	Problemas técnicos en la red de comunicaciones, lo que genera retrasos en las actividades y hasta parálisis en los procesos.
Hurto o Vandalismo	Se refiere a actos delictivos que ocasionan robos de activos de la información y/o actos vandálicos para sabotear los procesos de las empresas publicas
Malware	Es un software código malicioso diseñado para causar daño a los dispositivos y la información. Entre estos tipos de programas, se encuentra spyware, ransomware, rootkits y muchos más.
Falta de capacitación	Hace referencia a la falta de capacitación o entrenamiento del personal de la empresa, en la gestión de algunas herramientas de software o en la manipulación de hardware que puede generar daño con su manipulación.
Procedimientos desactualizados	Se refiere a que los procedimientos no cuentan con la documentación justificada de cada una de las actividades y/o procesos dentro de las áreas que componen las organizaciones.
Comportamiento no ético	Conductas inapropiadas de los usuarios tanto externos como internos, y que pueden llegar a atentar contra los activos de la información.
Factores ambientales	Es cualquier factor que proviene del medio ambiente, como temperaturas, lluvias, entre otros y puede ocasionar daños en los activos.
Orden público	Se pueden hacer una asonada en las instalaciones físicas de la empresa y puede ocasiones daños en la infraestructura tecnológica
Software desactualizado	Sistema operativo desactualizado, firmware desactualizado
Falta de monitoreo en la infraestructura de TI	Hace referencia a la falta de seguimiento de parámetros críticos en la infraestructura de software y hardware.
Incumplimiento del cronograma	Hace relación al incumplimiento de las actividades planeadas, generadas por el ausentismo laboral, lo que genera retraso en el proceso.

Fuente: elaboración trabajo grupo

A continuación, en el cuadro 19, se identificaron las vulnerabilidades en virtud del tipo de activo.

Cuadro 13. Vulnerabilidades identificadas

Tipo de Activo	Vulnerabilidad
Hardware	Falta de mantenimiento
	Sobrecarga de trabajo
	Fallas en las conexiones eléctricas
	Falta de UPS
	Falla en el suministro de energía alterna
	No existen planes de continuidad y recuperación
Software	Contraseñas débiles o predeterminadas
	Inadecuada gestión o protección de contraseñas
	Configuración predeterminada de servicios
	No existen copias de seguridad
	Software desactualizado
	Aplicaciones sin control de acceso
	Revisión de actualizaciones
	Falta de directivas de grupo
	Falta de antivirus
	No existen planes de continuidad y recuperación
	Falta de documentación/ciclo de vida
Servicios	Servicios no administrados
	Servicios mal configurados o por defecto
Red	Conexiones no controladas
	Falta de administración
	Falta de Documentación y procedimientos
	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
	Falta de gestión en las políticas
	Administración de red inadecuada
	Conexiones mal estructuradas
Personas	Entrenamiento Insuficiente
	Trabajo no supervisado
	Roles y responsabilidades no establecidas
	Falta de sensibilización en seguridad informática
	Errores humanos
	Planes de Contingencia para la realización de actividades
Instalaciones	Falta de Controles de acceso
	Falta de monitoreo factores críticos (temperatura, eléctrica y respaldo)
	Malas Condiciones eléctricas
	Desastre natural
	Falta de mantenimiento a la infraestructura
	Procedimientos no definidos
	No existen infraestructuras redundantes

Fuente: elaboración grupo de trabajo

A continuación, en el cuadro 20, se relacionan las amenazas y las vulnerabilidades de acuerdo con los tipos de riesgos asociados a la seguridad digital: perdida de confidencialidad, perdida de integridad y perdida de la disponibilidad.

Cuadro 14. Riesgos asociados a la seguridad digital IBAL

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades
GC-001	Dispositivos Celulares	Pérdida de disponibilidad	Hurto o vandalismo	Errores humanos
GC-002	Catastro de suscriptores	Pérdida de integridad	Acceso no autorizado	
GC-003	Recurso Humano	Pérdida de disponibilidad	Incumplimiento del cronograma	Falta de Planes de Contingencia para la realización de actividades
		Pérdida de Integridad	Comportamiento no ético	Trabajo no supervisado
				Falta de sensibilización en seguridad informática
GC-004	Documentos en papel	Pérdida de disponibilidad	Destrucción de información	Errores humanos
		Perdidas de confidencialidad	Comportamiento no ético	Trabajo no supervisado
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
		Pérdida de disponibilidad	Fallas en la comunicación	Administración de red inadecuada
				Conexiones mal estructuradas
				No existen planes de continuidad y recuperación
		Pérdida de la integridad	Fallas en el software	Software desactualizado
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
		Pérdida de disponibilidad	Destrucción de información	No existen planes de continuidad y recuperación
				Servicios mal configurados o por defecto
GT-003	Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida
		Pérdida de confidencialidad	Acceso no autorizado	Aplicaciones sin control de acceso
GT-004	Base de datos Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Malware	Servicios mal configurados o por defecto
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Malware	Servicios mal configurados o por defecto
GT-007	Servidor de Aplicaciones INTRANET	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Malware	Servicios mal configurados o por defecto
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida
GT-008	Servidor de Base de datos INTRANET	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Malware	Servicios mal configurados o por defecto
GT-009	Canales de Datos	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
GT-010	Servicio de Internet	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
GT-011	Firewall	Pérdida de confidencialidad	Software desactualizado	Revisión de actualizaciones
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Falta de monitoreo en la infraestructura de TI	Falta de gestión en las políticas
		Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas
				Falta de UPS

				Falla en el suministro de energía alterna
GT-012	Switch Core Comunicaciones	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-013	Switch Core Servidores	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-014	Computadores usuarios finales	Pérdida de confidencialidad	Malware	Software desactualizado
		Pérdida de disponibilidad	Fallas en las comunicaciones	Administración de red inadecuada
			Fallas en el software	Falta de directivas de grupo
			Fallas en el Hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
GT-015	Antivirus	Pérdida de confidencialidad	Malware	Software desactualizado
			Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos
				Falta de monitoreo factores críticos
			Fallas en hardware	Falta de mantenimiento a la infraestructura
				Sobrecarga de trabajo
				Fallas en las conexiones eléctricas
				No existen infraestructuras redundantes
				Falta de UPS
				Falla en el suministro de energía alterna
				Desastre natural
			Acceso no autorizado	Falta de Controles de acceso
			Fallas en las comunicaciones	Falta de Documentación y procedimientos
			Procedimientos desactualizados	Falta de Documentación y procedimientos

Fuente: elaboración grupo de trabajo

1.1.5.3 Valoración del riesgo. En esta fase de la administración del riesgo se estableció la probabilidad de ocurrencia de los riesgos identificados y el nivel de consecuencia o impacto, con el fin de identificar la zona de riesgo inicial, para el desarrollo de esta valoración se tuvo en cuenta el nivel de frecuencia que se observa en el cuadro 21.

Cuadro 15. Probabilidad de ocurrencia del riesgo

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	0% - 20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	20.01% - 40%
Media	La actividad que coxnlleva el riesgo se ejecuta de 24 a 500 veces por año	40.01% - 60%

Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	60.01% - 80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	80.01% - 100%

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. página 39.

Con el fin de determinar la probabilidad de ocurrencia del riesgo, se realizó el análisis del número de veces que se realiza la actividad con relación a cada uno de los activos de información como se muestra en el cuadro 22.

Cuadro 16. Actividades relacionadas con el activo

ID Activo	Nombre del Activo	Nro de Veces aproximado que se ejecuta la actividad por mes	Descripción (fórmula)
GC-001	Dispositivos Celulares	264.51	Total, lecturas suscriptores: 158,706 (Agosto/2021) Lecturas por Operario: 600 registros día Fórmula: 158,706/600
GC-002	Catastro de suscriptores	171.43	Total, novedades catastro de suscriptores: 1,200 (cambios de uso, estrato) Total, Ciclos facturación: 7 Fórmula: 1,200/7
GC-003	Recurso Humano	1,300	Días laborales en el mes: 26 Número de Operarios Lecturas: 50 Fórmula: 26x50
GC-004	Documentos en papel	15,000	Total de actividades de lecturas realizadas en papel.
GT-001	Solin CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-002	Base de datos SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-003	Intranet	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-004	Base de datos Intranet	14	Total, Ciclos facturación: 7

			Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-007	Servidor de Aplicaciones INTRANET	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-008	Servidor de Base de datos INTRANET	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-009	Canales de Datos	130	Número de sede: 5 Días laborales en el mes: 26 Fórmula: 7 x 26
GT-010	Servicio de Internet	264.51	Total, lecturas suscriptores: 158,706 Lecturas por Operario: 600 registros día Fórmula: 158,706/600
GT-011	Firewall	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30
GT-012	Switch Core Comunicaciones	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30
GT-013	Switch Core Servidores	234	Número de Servidores físicos y virtuales: 9 Días laborales en el mes: 26 Fórmula: 9 x 26
GT-014	Computadores usuarios finales	6,266	Inventario de Computadores: 241 Días laborales en el mes: 26 Fórmula: 241 x 26
GT-015	Antivirus	6,500	Inventario de Computadores: 250 Días laborales en el mes: 26 Fórmula: 250 x 30
GT-016	Datacenter	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30

Fuente: elaboración grupo de trabajo

Para medir el impacto del riesgo, se definieron los siguientes criterios en el caso que se llegue a materializar dichos riesgos. Ver cuadro 23.

Cuadro 17 Niveles de medición del Impacto del riesgo

AFECTACION		IMPACTO	
Económica	**Reputacional**	**Cualitativo**	**Cuantitativo**
Afectación en SMLMV	El riesgo afecta la imagen de:		
Menor a 10	Alguna área de la organización	20%	Leve
Entre 10 y 50	La entidad internamente, la junta directiva y/o de proveedores	40%	Menor
Entre 50 y 100	La entidad frente a algunos usuarios en referencia al logro de los objetivos	60%	Moderado
Entre 100 y 500	La entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%	Mayor
Mayor a 500	La entidad a nivel nacional, con divulgación a todo el país	100%	Catastrófico

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. página 40.

De acuerdo con el cuadro 24, se calculó el nivel de impacto en caso de materializarse un riesgo debido a un incidente de seguridad.

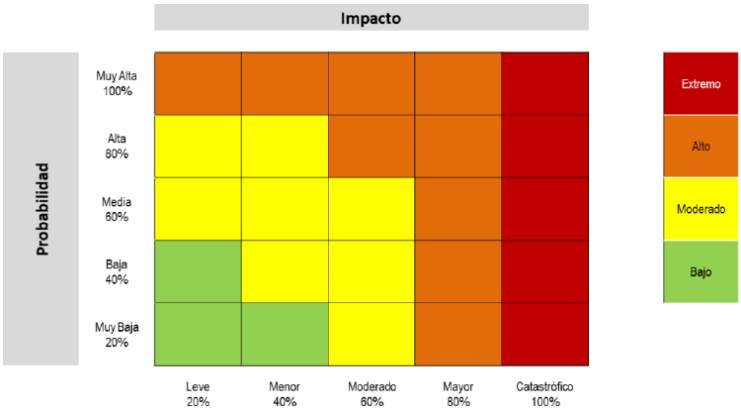
Cuadro 18. Nivel de impacto en caso de materializarse el riesgo

ID Activo	Nombre del Activo	Afectación Económica aproximada	Descripción (formula)
GC-001	Dispositivos Celulares	$ 1,000,000	Valor de un dispositivo móvil año 2021.
GC-002	Catastro de suscriptores	$42,000,000	Total, novedades catastro de suscriptores: 1,200 en el mes. Valor promedio de 1 factura: $ 35,000
GC-003	Recurso Humano	$ 0	Aunque el personal operativo no esté disponible, el IBAL cuenta con mecanismos de ley que le permitan liquidar una factura con consumos promedios por eventualidad.
GC-004	Documentos en papel	$ 40,000	Salario Mensual operario: $ 1,200,000 Días del Mes: 30
GT-001	Solin CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-002	Base de datos SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-003	Intranet	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-004	Base de datos Intranet	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-007	Servidor de Aplicaciones INTRANET	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-008	Servidor de Base de datos INTRANET	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-009	Canales de Datos	$ 0	Si se materializa el riesgo se puede realizar las actividades en sede principal del IBAL
GT-010	Servicio de Internet	$ 0	Si se materializa el riesgo se puede realizar las actividades en sede principal del IBAL
GT-011	Firewall	$ 30,000,000	Precio del appliance y configuración de las políticas y servicios
GT-012	Switch Core Comunicaciones	$ 3,000,000	Precio del swtich capa 2
GT-013	Switch Core Servidores	$ 3,000,000	Precio del swtich capa 2
GT-014	Computadores usuarios finales	$ 4,500,000	Valor del computador o de la reconfiguración o de las piezas afectadas.
GT-015	Antivirus	Moderado	Teniendo en cuenta que el riesgo al no tener una solución protección contra virus, se pueden generar daños en los computadores de los usuarios finales, la cual con el tiempo se puede volver a reconstruir. Con relación a los servidores, el riesgo de afectación por malware, generaría la aplicación de los planes de contingencia, lo cual paralizaría los procesos por 5 días aproximadamente, afectando la imagen de la entidad con los usuarios del servicio.
GT-016	Datacenter	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000

Fuente: Elaboración grupo de trabajo

Para estimar el nivel de riesgo inicial – inherente, se realizó a través de la determinación de la probabilidad y el impacto que puede ocasionar la materialización del riesgo, para esto se tuvo en cuenta el cuadro 25, de acuerdo con la guía del DAFP.

Cuadro 19. Matriz de Calor Inherente



Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. ANEXO 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS. Versión 1. Página 82.

Basado en los criterios anteriormente mencionados, se procedió a determinar la probabilidad y el impacto que puede ocasionar la materialización de los riesgos anteriormente mencionados durante la ejecución de las actividades del proceso gestión tecnológica, ver cuadro 26.

Cuadro 20. Zona de riesgo inherente

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo
GC-001	Dispositivos Celulares	Pérdida de disponibilidad	Hurto o vandalismo	Errores humanos	Alta (80%)	Leve (20%)	Moderado
GC-002	Catastro de suscriptores	Pérdida de integridad	Acceso no autorizado	Falta de Planes de Contingencia para la realización de actividades	Alta (80%)	Mayor (80%)	Alto
GC-003	Recurso Humano	Pérdida de disponibilidad	Incumplimiento del cronograma	Trabajo no supervisado	Muy Alta (100%)	Leve (20%)	Alto
		Pérdida de Integridad	Comportamiento no ético	Falta de sensibilización en seguridad informática			
				Errores humanos			
GC-004	Documentos en papel	Pérdida de disponibilidad	Destrucción de información	Trabajo no supervisado	Muy Alta (100%)	Leve (20%)	Alto
		Perdidas de confidencialidad	Comportamiento no ético	Inadecuada gestión o protección de contraseñas	Muy Alta (100%)	Leve (20%)	Alto
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Administración de red inadecuada	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Fallas en la comunicación	Conexiones mal estructuradas			
				Software desactualizado			
				Inadecuada gestión o protección de contraseñas			
				Servicios mal configurados o por defecto			
		Pérdida de la integridad	Fallas en el software	Inadecuada gestión o protección de contraseñas			
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Falta de documentación/ciclo de vida	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Destrucción de información	Aplicaciones sin control de acceso			
				Inadecuada gestión o protección de contraseñas			
GT-003	Intranet	Pérdida de disponibilidad	Acceso no autorizado	Falta de mantenimiento	Media (60%)	Leve (20%)	Moderado
				Fallas en las conexiones eléctricas			
		Pérdida de la integridad	Fallas en el software	Falta de UPS			
		Pérdida de confidencialidad	Acceso no autorizado	Falla en el suministro de energía alterna			
GT-004	Base de datos Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Leve (20%)	Moderado
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento	Media (60%)	Catastrófico (100%)	Extremo
				Fallas en las conexiones eléctricas			
				Falta de UPS			
				Falla en el suministro de energía alterna			
			Malware	Falta de documentación/ciclo de vida			
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo
			Malware	Servicios mal configurados o por defecto			
GT-007	Servidor de Aplicaciones INTRANET	Pérdida de disponibilidad	Fallas en hardware	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones	Media (60%)	Leve (20%)	Moderado
				Falta de acuerdos de nivel de servicio (ANS) en comunicaciones			
				Revisión de actualizaciones			
				Inadecuada gestión o protección de contraseñas			
			Malware	Falta de gestión en las políticas			
		Pérdida de la integridad	Fallas en el software	Fallas en las conexiones eléctricas			
GT-008	Servidor de Base de datos INTRANET	Pérdida de disponibilidad	Acceso no autorizado	Falta de UPS	Media (60%)	Leve (20%)	Moderado
			Malware	Falla en el suministro de energía alterna			
GT-009	Canales de Datos	Pérdida de disponibilidad	Factores ambientales	Fallas en las conexiones eléctricas	Alta (80%)	Leve (20%)	Moderado
GT-010	Servicio de Internet	Pérdida de disponibilidad	Factores ambientales	Falta de UPS			

GT-011	Firewall	Pérdida de confidencialidad	Software desactualizado	Falla en el suministro de energía alterna	Muy Alta (100%)	Leve (20%)	Alto
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas			
			Falta de monitoreo en la infraestructura de TI	Fallas en las conexiones eléctricas			
		Pérdida de disponibilidad	Fallas en el hardware	Falta de UPS			
				Falla en el suministro de energía alterna			
				Inadecuada gestión o protección de contraseñas			
GT-012	Switch Core Comunicaciones	Pérdida de disponibilidad	Fallas en el hardware	Software desactualizado	Muy Alta (100%)	Leve (20%)	Alto
				Administración de red inadecuada			
				Falta de directivas de grupo			
			Acceso no autorizado	Falta de mantenimiento			
GT-013	Switch Core Servidores	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas	Alta (80%)	Leve (20%)	Moderado
				Falta de UPS			
				Falla en el suministro de energía alterna			
			Acceso no autorizado	Software desactualizado			
GT-014	Computadores usuarios finales	Pérdida de Confidencialidad	Malware	Falta de Documentación y procedimientos	Muy Alta (100%)	Leve (20%)	Alto
		Pérdida de disponibilidad	Fallas en las comunicaciones	Falta de Documentación y procedimientos			
			Fallas en el software	Falta de monitoreo factores críticos			
			Fallas en el Hardware	Falta de mantenimiento a la infraestructura			
				Sobrecarga de trabajo			
				Fallas en las conexiones eléctricas			
				No existen infraestructuras redundantes			
GT-015	Antivirus	Pérdida de confidencialidad	Malware	Falta de UPS	Muy Alta (100%)	Moderado (60%)	Alto
			Falta de monitoreo en la infraestructura de TI	Falla en el suministro de energía alterna			
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Desastre natural	Muy Alta (100%)	Catastrófico (100%)	Extremo
				Falta de Controles de acceso			
			Fallas en hardware	Falta de Documentación y procedimientos			
			Acceso no autorizado				
			Fallas en las comunicaciones				
			Procedimientos desactualizados				

Fuente: Elaboración grupo de trabajo

1.1.5.4 Controles asociados a la seguridad de la información. De acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades pública de la DAFP, se tiene que emplear como mínimo los controles del anexo 4 Del "Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas", referidos en el capítulo 5 páginas 29 a 38, siempre y cuando se ajusten al análisis de riesgos.

Como primera medida para identificar los controles a implementar, se van a tomar los riesgos qué resultaron en la zona de riesgo extremo (ver cuadro 27), debido al nivel de impacto que alguno de ellos puede generar sobre la información y la continuidad del negocio, a su vez el impacto económico que generaría la materialización de estos para el IBAL.

Adicionalmente, como se logró evidenciar en el resultado de la evaluación de los controles con la herramienta del autodiagnóstico de MINTIC (ver cuadro 3), el ***dominio A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio,*** obtuvo un puntaje de 14, lo que demuestra que debe tomarse como referencia para diseñar los controles que permitan reducir la brecha de seguridad con relación a la ISO/IEC 27001:2013.

Cuadro 21. Zona de riesgo inherente extremo para la selección de controles

ID Activo	Nombre del Activo	Riesgo	Amenazas	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Fallas en la comunicación			
		Pérdida de la integridad	Fallas en el software			
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Destrucción de información			
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Media (60%)	Catastrófico (100%)	Extremo
			Malware			
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
			Malware			
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Muy Alta (100%)	Catastrófico (100%)	Extremo
			Fallas en hardware			
			Acceso no autorizado			
			Fallas en las comunicaciones			
			Procedimientos desactualizados			

Fuente: Elaboración grupo de trabajo

A continuación, en el cuadro 28, se listan los controles que se deben de implementar para mitigar los riesgos identificados (Zona de Riesgo: Extremo), según el Anexo A del estándar ISO/IEC 27001:2013, los cuales se ajustan al análisis de riesgos realizados en la Dirección Comercial y el grupo de Gestión Tecnológica del IBAL.

Cuadro 22. Controles a implementar en la zona de riesgo inherente extremo

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo	ACTIVIDAD DE CONTROL	Soporte
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.9.1.1** Política de control de acceso **A.13.1.1** Controles de redes **A.14.2.7** Desarrollo contratado externamente	**A.9.1.1** En la política de seguridad y privacidad de la información, se debe establecer una política de control de acceso más coherente con el nivel del riesgo, con el fin de minimizarlo. **A.13.1.1** Se deben implementar directrices relacionadas con la gestión de seguridad de las redes, encaminadas a establecer las responsabilidades y procedimientos para la gestión de equipos. **A.14.2.7** Se deben implementar directrices relacionadas con el desarrollo de software contratado externamente, con el fin de realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables.
		Pérdida de disponibilidad	Fallas en la comunicación	Administración de red inadecuada					
				Conexiones mal estructuradas					
		Pérdida de la confidencialidad	Fallas en el software	Software desactualizado					
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.9.1.1** Política de control de acceso **A.12.3.1** Respaldo de información	**A.9.1.1** En la política de seguridad y privacidad de la información, se debe establecer una política de control de acceso enfocada en gestionar los usuarios que se conectan a la base de datos. **A.12.3.1** Se deben implementar procedimientos para la verificación de la funcionalidad de las copias de respaldo, ante un evento, así como los roles y responsables de realizar esta actividad.
		Pérdida de disponibilidad	Destrucción de información	No existen planes de continuidad y recuperación					
				Servicios mal configurados o por defecto					
GT-005	Servidor de Aplicacione	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento	Media (60%)	Catastrófico (100%)	Extremo	**A.11.2.4** Mantenimiento	**A.11.2.4** Se deben

	s SOLIN CLOUD ERP			Fallas en las conexiones eléctricas				de equipos **A.12.6.1** Gestión de las vulnerabilidades técnicas	implementar procedimientos para la elaboración de los mantenimientos periódicos de los servidores, según las especificaciones del fabricante. Se debe llevar registro de fallas o sospechas con el fin de planear mantenimientos preventivos o correctivos. **A.12.6.1** Se deben implementar procedimientos que permitan la detección y análisis de vulnerabilidades al sistema operativo y los servicios que se tengan configurados.
				Falta de UPS					
				Falla en el suministro de energía alterna					
			Malware	Servicios mal configurados o por defecto					
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.12.6.1** Gestión de las vulnerabilidades técnicas	**A.12.6.1** Se debe llevar registro de fallas o sospechas con el fin de planear mantenimientos preventivos o correctivos. **A.12.6.1** Se deben implementar procedimientos que permitan la detección y análisis de vulnerabilidades al sistema operativo y los servicios que se tengan configurados.
			Malware	Servicios mal configurados o por defecto					
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos	Muy Alta (100%)	Catastrófico (100%)	Extremo	**A.11.1.1** Perímetro de seguridad física. **A.11.2.1** Ubicación y protección de los equipos. **A.11.2.2** Servicios de suministro. **A.11.2.4** Mantenimiento de equipos.	**A.11.1.1** En la política de seguridad y privacidad de la información, se debe establecer las directrices para el control de acceso a los funcionarios a las instalaciones de procesamiento de información crítica, así como los controles físicos de entrada. . **A.11.2.1** Se deben implementar procedimientos relacionados con los controles para minimizar el
				Falta de monitoreo factores críticos					
			Fallas en hardware	Falta de mantenimiento a la infraestructura					
				Sobrecarga de trabajo					
				Fallas en las conexiones eléctricas					
				No existen infraestructuras redundantes					
				Falta de UPS					
				Falla en el suministro de energía alterna					
			Acceso no autorizado	Falta de Controles de acceso					
			Fallas en las comunicaciones	Falta de Documentación y procedimientos					

			Procedimientos desactualizados	Falta de Documentación y procedimientos					riesgo de amenazas físicas y ambientales, así como el seguimiento de las condiciones críticas de este entorno. **A.11.2.2** Se deben llevar un registro con el fin de validar el funcionamiento que brindan el suministro eléctrico **A.11.2.4** Se deben implementar procedimientos para la elaboración de los mantenimiento periódicos a los equipos que se encuentran en el centro de datos según las especificaciones del fabricante. Se debe llevar registro de fallas o sospechas con el fin de planear mantenimientos preventivos o correctivos.

Fuente: Elaboración grupo de trabajo