DISEÑO DEL PLAN DE CONTINGENCIA PARA EL SERVICIO TI “CONTROL DE ACCESO” OFRECIDO POR GROW DATA

JONNATHAN DAVID TRIANA BOTÍA
MANUEL ANTONIO CASTRO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

DISEÑO DEL PLAN DE CONTINGENCIA PARA EL SERVICIO TI “CONTROL DE ACCESO” OFRECIDO POR GROW DATA

JONNATHAN DAVID TRIANA BOTÍA
MANUEL ANTONIO CASTRO

Proyecto de grado para la obtención del título de especialización en seguridad informática

Asesora proyecto de grado
Ingeniera Lorena Ocampo

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA): proceso de análisis de actividades identificando el efecto que podría tener sobre ellas la interrupción de su gestión y desarrollo normal[1].

ANÁLISIS DE RIESGO: proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo (AMN ISO Guía 73, 2009)[2].

AMENAZA: se entiende como cualquier causa potencial de un incidente no deseado, que puede provocar daños graves a un sistema de información, redes, instalaciones o a la Entidad (NTC-ISO/IEC:27000, 2018)[3].

CONTINUIDAD DEL NEGOCIO: capacidad de la Entidad para continuar desarrollando y entregando los servicios en un nivel aceptable predefinido, luego de un incidente[4].

DETECCIÓN DE INTRUSOS: método para analizar la información referente a las redes y los sistemas de información, para determinar si se ha producido una violación de seguridad (CNSSI No. 4009, 2015)[5].

DISPONIBILIDAD: comprende la capacidad de los usuarios para acceder, utilizar o dar tratamiento a la información autorizada por la Entidad, en una ubicación determinada y en un formato correcto (NTC-ISO/IEC:27000, 2018)[6].

DRP (DISASTER RECOVERY PLAN / PLAN DE RECUPERACIÓN DE DESASTRE): el DRP suministra los procedimientos detallados para facilitar la recuperación de las capacidades en sitio alterno. Normalmente está enfocado en Tecnologías de la Información (en adelante TI) y limitado a interrupciones mayores con efectos a largo plazo (ISO/IEC:27031, 2011)[7].

EVENTO: distingue los aspectos o alteración de un conjunto particular de situaciones (Accidentes, incidentes y circunstancias peligrosas) (NTC-ISO:31000, 2018)[8].

---

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019, International Organization for Standardization, 2019.

[2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Gestión del riesgo - Vocabulario. Asociación MERCOSUR de Normalización (AMN).Asociación MERCOSUR de Normalización (AMN), 2009.

[3] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27000. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.

[4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019

[5] NATIONAL SECURITY AGENCY (NSA). Committee on National Security Systems (CNSS).

[6] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27000.

[7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC:27031. Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de la información y la comunicación para la continuidad del negocio.

[8] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO:31000. Gestión del Riesgo. Principios y Directrices.

EVENTO CATASTRÓFICO: aquellas situaciones con la capacidad de interrumpir la continuidad de las actividades del negocio generando impactos críticos, daños mayores y/o no recuperables para la Entidad[9].

INCIDENTE: situación que puede ser o podría dar lugar a una interrupción, pérdidas, emergencias o crisis[10].

INFRAESTRUCTURA: sistemas, equipos y servicios necesarios para la operación de una Entidad[11].

ISO: Organización Internacional de Normalización[12].

PLAN DE CONTINUIDAD DEL NEGOCIO: procedimiento documentado que guía a la Entidad para reaccionar ante incidentes naturales y/o de factor humano, que lleven a la interrupción directa de la operación, identificando los niveles mínimos en los cuales la Entidad pueda garantizar la continuidad de la operación (International Organization for Standardization (ISO), 2018)[13].

PLAN DE RESPUESTA A INCIDENTES: el plan incluye procedimientos documentados y lineamientos para la definición de la criticidad de los incidentes, los procesos de presentación de informes y escalado, y los procedimientos de recuperación (International Organization for Standardization (ISO), 2018)[14].

RESPUESTA A INCIDENTES: la respuesta a un desastre u otro evento significativo que pueda afectar de manera significativa a la empresa, su gente, o su capacidad de funcionar de manera productiva. Puede incluir la evacuación de instalaciones, iniciando un plan de recuperación de desastres (DRP), la realización de la evaluación de daños y otras medidas necesarias para llevar una empresa a un estado más estable (International Organization for Standardization (ISO), 2018)[15].

RIESGO: posibilidad de que una amenaza, aproveche o explote una vulnerabilidad para causar una pérdida o daño en un activo de información. Esto suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (NTC-ISO/IEC:27000, 2018)[16].

---

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019

[10] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019

[12] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019

[13] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. ISO:22301. Sistemas de Gestión y Continuidad del Negocio.

[14] ISO:22301. Sistemas de Gestión y Continuidad del Negocio.

[15] ISO:22301. Sistemas de Gestión y Continuidad del Negocio.

[16] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27000. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.

SEGURIDAD PERIMETRAL: se define como el perímetro imaginario o línea, que separa una Entidad (sus computadoras, servidores, etc.) de otras redes (generalmente el internet) (NTC-ISO/IEC:27002, 2013)[17].

SGCN (SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO): parte de la gestión general para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de la continuidad del negocio (International Standards. Societal security. Business continuity management systems. Requirements, 2019)[18].

[17] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27002. Controles de Seguridad

[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO 22301. International Standards. Society security. Business continuity management systems. Requirements

INTRODUCCIÓN

Grow Data es una compañía experta en integración de data y tecnología para acompañar a las organizaciones públicas o privadas en su proceso de transformación digital. Articulando los objetivos del negocio, los sistemas, aplicaciones, la información y toda su infraestructura tecnológica a través de modelos de pensamiento ágil y consultoría avanzada[19]. La organización se centra en tres líneas de negocio donde se abarcan los servicios ofrecidos a las diferentes entidades del sector público y/o privado, las cuales son:

Datos y sistemas de información: Servicio de especialistas en Business Intelligence, procesos de arquitectura y Data Science que permiten capitalizar oportunidades de crecimiento.

Servicios Consultivos: Desarrollo de ecosistemas de Arquitectura empresarial y Consultoría en materia de TIC a nivel gerencial, estratégico y operativo soportados en procesos avalados por organismos nacionales e internacionales.

Servicios de TI: Servicios que se alinean a los requerimientos tecnológicos de los clientes, adaptándose a sus necesidades de seguridad, apoyo estratégico e infraestructura ayudando a consolidar su estrategia de negocio y a cumplir con su misionalidad.

De esta última línea de negocio, Grow Data ofrece el servicio TI de “Control de acceso”, donde gestionan soluciones de videovigilancia, video analítica como controles de acceso y circuitos cerrados de televisión.

En la actualidad Grow Data identifica la necesidad de poder asegurar la continuidad en la prestación del servicio de Control de Acceso, desarrollando un plan de contingencia para el servicio TI “Control de acceso”, el cual es el servicio donde convergen los mecanismos de control de acceso basados en el reconocimiento de identidad de aquellas personas que solicitan ingreso a las instalaciones físicas de las entidades a la cuales Grow Data ofrece este servicio.

Por consiguiente, en este proyecto se presentan las fases que abarcan el cumplimiento de los objetivos propuestos entre los cuales se encuentran el levantamiento de activos de información, análisis de riesgos de los activos de información, definición del tratamiento de los riesgos identificados, levantamiento del análisis de impacto del negocio, medición de los tiempos de recuperación (RPO, RTO, MAO, MTD), definición de las fases de activación del plan de contingencia y la definición de las estrategias de contingencia, haciendo uso de diferentes

[19] GROW DATA. Grow Data misión [en línea]. Obtenido de https://growdata.com.co/nosotros/ el 22 de 11 de 2021.

herramientas donde se incluyen entrevistas, documentos internos y plantillas de levantamiento de información (Activos, Riesgos, BIA), etc. y además utilizando las mejores prácticas y marcos de referencia como lo son la norma ISO 31000:2018 y la norma ISO/IEC 27001:2013.

Con esto, se ofrece el plan de contingencia a Grow Data para responder adecuadamente al momento de reanudar las operaciones e identificar controles del servicio TI “Control de Acceso”, ofreciendo un valor agregado al momento de exponer este servicio a sus potenciales clientes.

1. JUSTIFICACIÓN

De acuerdo con el proceso de criticidad que apoya el Sistema "Biostar2", se identifica la necesidad de contar con un diseño del plan de contingencia, el cual apoya la misionalidad del servicio TI definido como "Control de Acceso."

Teniendo en cuenta que la seguridad física y el control de acceso a las diferentes instalaciones de los posibles clientes que se encuentran ubicados en la ciudad de Bogotá D.C., se ha vuelto un tema bastante importante para responder y buscar seguridad tanto de la información como del personal, es necesario generar un plan de contingencia con el que Grow Data busca garantizar la continuidad y el restablecimiento del servicio TI ofrecido, ya que la intermitencia y la no entrega del servicio genera un alto riesgo para los clientes que obtienen el servicio TI, al no poder controlar quién, en dónde o cómo se ingresa a sus instalaciones.

Por lo tanto, el diseño del plan de contingencia ayudará a que la organización busque el mejoramiento continuo y pueda estar preparada de una manera más formal, para restablecer los servicios de "Control de Acceso" ante cualquier tipo de desastre o evento.

El beneficio de contar con el diseño del plan de contingencia es ayudar a Grow Data a formalizar sus procedimientos y actividades que favorezcan en la búsqueda de responder adecuadamente al momento de reanudar las operaciones del servicio TI "Control de Acceso", ofreciendo un valor agregado al momento de presentar este servicio a sus potenciales clientes.

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

La problemática para Grow Data se centra en que no se cuenta con la capacidad de atender un incidente cuando este se materializa y que afecte la operación normal del servicio de TI “Control de Acceso” como resultado, la entrega de este a sus clientes y respuestas han sido lentas y poco efectivas para contrarrestar los posibles impactos negativos.

Dicho lo anterior y teniendo en cuenta la misionalidad la cual dicta “garantizar la plena identificación del personal que accede a las instalaciones controlando donde y como se ingresa salvaguardando la información generada del servicio TI”; Si se llegara a materializar un desastre y/o incidente que impida su operación normal, Grow Data no tendría la capacidad de reaccionar de una manera adecuada, derivando en posibles consecuencias negativas para el cliente al cual se le presta el servicio TI, viéndose afectado en su reputación, económicamente y comprometiendo la seguridad física del mismo.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son las actividades y/o estrategias que se deben establecer para que Grow Data de continuidad al servicio TI "Control de Acceso" en las instalaciones ante la materialización de un desastre o evento que afecte su operación?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el plan de contingencia para el servicio TI “Control de Acceso” ofrecido por Grow Data.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar levantamiento de activos de información asociados al servicio TI “Control de Acceso” de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MINTIC.
- Realizar un análisis de riesgos de los activos de información a los que se encuentra expuesto el servicio TI “Control de Acceso” de acuerdo con la metodología de análisis de riesgos de la norma ISO 31000:2018 y MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.
- Definir el plan de tratamiento de riesgos de la seguridad de la información con base en el Anexo A de la norma ISO/IEC 27001.2013.
- Realizar el levantamiento de información del Análisis de Impacto al Negocio (BIA) de acuerdo con la Guía para realizar Análisis de Impacto al Negocio de MINTIC.
- Medir el RPO (Punto Objetivo de Recuperación) y el RTO (Tiempo Objetivo de Recuperación) de acuerdo con la Guía para realizar Análisis de Impacto al Negocio de MINTIC.
- Medir el MAO (Interrupción Máxima Aceptable) y el MTD (Tiempo Máximo Tolerable) de acuerdo con la Guía para realizar Análisis de Impacto al Negocio de MINTIC.
- Definir las fases de activación del plan de contingencia del servicio TI “Control de Acceso” ofrecido por Grow Data de acuerdo con la norma ISO 22301:2019.
- Definir estrategias de contingencia para los escenarios planteados donde Grow Data ofrece el servicio TI “Control de Acceso” con base en la norma ISO 22301:2019.

4. MARCO TEÓRICO

En un mundo tan globalizado los avances tecnológicos han marcado a la continuidad del negocio dentro de las organizaciones como un factor indispensable para el logro de sus objetivos, estableciendo la importancia que las tecnologías de la información y las comunicaciones (TIC) han adquirido para facilitar la realización de trabajos y actividades que anteriormente parecían imposibles.

De acuerdo con lo anterior, es necesario identificar las diferentes fases para la elaboración de un plan de contingencia que establezca las estrategias y procedimientos preventivos y reactivos que permitan un rápido retorno a la operación normal, permitiendo así que Grow Data recupere en un nivel aceptable después de una interrupción no prevista el servicio TI “Control de acceso”.

En cuanto a este documento busca diseñar el plan de contingencia que permita abarcar todas las posibles amenazas a los que se encuentran expuestos los activos críticos que apalancan el servicio TI “Control de acceso” para tener una respuesta planificada a estas y acorde a los recursos disponibles con los que cuenta Grow Data.

Para poder desarrollar este plan primero se debe establecer de manera clara la definición de plan de contingencia, el cual no es más que un documento que busca prevenir y reaccionar, estructurado estratégica y operativamente para ayudar a controlar una situación de emergencia y a minimizar sus impactos negativos que puedan afectar a Grow Data.

Actualmente, existen diversas metodologías, frameworks, buenas prácticas, etc., que ayudan a las entidades u organizaciones que se encuentran interesadas en diseñar, y/o implementar las diferentes actividades, que les ayuden a poder asegurar la continuidad de los servicios ofrecidos, ya sea en el ámbito privado o público.

En los siguientes capítulos, se describen las metodologías seleccionadas que ayudan a dar forma al proyecto de investigación, y las cuales brindan el sustento académico y normativo vigente para apalancar el desarrollo del presente proyecto.

4.1 PLAN DE CONTINGENCIA PARA EL SERVICIO TI

Un plan de contingencia para el servicio o sistema de TI es entendido como un conjunto de medidas provisionales que se implementan para recuperar los servicios de TI después de la ocurrencia de una emergencia, interrupción o evento disruptivo de los sistemas de la empresa u organización en cuestión. A continuación, se presentan algunos pasos que se pueden seguir para implementar un plan de contingencia para sistemas TI. Dichos planes son importantes entre otras cosas,

porque si bien un seguro “puede cubrir los costos materiales de los activos de las empresas en caso de un desastre, robo u otras amenazas, no servirá para recuperar la información almacenada perjudicando a la entidad”[20]

En este sentido, algunos de los pasos que se pueden seguir para implementar un plan de contingencia para sistemas TI son los siguientes: En primer lugar, analizar y prever los riesgos, ya que, en toda empresa, es importante identificar todos los posibles riesgos a los que está expuesta la infraestructura TI, para de esa manera poder prever cómo pueden mitigarse. Algunos riesgos que se tienen en este tipo de sistemas son la pérdida de datos, la interrupción del servicio, la falta de energía eléctrica, entre otros [21].

En segundo lugar, se deben establecer las estrategias de continuidad del servicio TI, una vez que se realiza la identificación de los riesgos, deben establecerse las estrategias de continuidad del servicio TI. Dichas estrategias pueden incluir acciones como la implementación de un sistema de respaldo, creación de planes de recuperación, generación de copias de seguridad periódicas, entre otros. Finalmente, deben adoptarse las medidas para garantizar la disponibilidad de los recursos críticos, como la energía eléctrica o las telecomunicaciones. En una gran diversidad de casos, dichos recursos pueden residir fuera del control de la organización, por lo que es importante tener un plan de contingencia efectivo para mitigar el riesgo de indisponibilidad del sistema y del servicio. Los plantes también pueden establecer un plan de comunicación en caso de contingencia de manera que se garantice que todos los miembros del equipo de trabajo se encuentran informados sobre la situación y sepan qué acciones seguir en caso de una interrupción del servicio[22].

4.2 ANÁLISIS DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN

Para el análisis de riesgos de los activos de información en las empresas, acción que ha ganado trascendencia e impulso en los últimos años debido a los avances tecnológicos, especialmente a partir de los años noventa, han surgido “Modelos de Gestión de Riesgos”, algunos generales como los estándares Australiano (AS/NZS 4630) e ISO/IEC 31000, y otros de carácter más específico, por ejemplo: Committee of Sponsoring Organizations (COSO), ISO 14000, ISO 22000, ISO 27005 y Occupational Health and Safety Advisory Services (OHSAS). [23] Para efectos de esta

[20] FERRUZOLA GÓMEZ, Enrique; DUCHIMAZA, Johanna, RAMOS HOLGUÍN, Johanna, ALEJANDRO, María Fernanda. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE Vol. 6, Nº 1, 2019, p.35
[21] VERDÚ FERNÁNDEZ, José Ignacio. Plan de contingencia de tecnologías de la información en entornos distribuidos. 2016. Tesis de Licenciatura.
[22] VERDÚ FERNÁNDEZ, José Ignacio.
[23] BEDÓN, Marcos.; UTRILLA, José.; ORTEGA, Juan. Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf, 2012.

investigación se hablará en los epígrafes siguientes sobre la norma ISO 31000:2018, la metodología Margerit, la norma ISO/IEC 27001:2013, norma ISO 22301:2019.

4.3 GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN – MINTIC

Mediante esta guía el Ministerio de Tecnologías de la Información y las Comunicaciones definen los lineamientos básicos que deben ser tenidos en cuenta por parte de los responsables de la seguridad de la información en Grow Data, para poner en marcha la gestión y clasificación de activos de información que apoyan la entrega del servicio TI “Control de Acceso”, con el fin de determinar que activos se encuentran bajo su responsabilidad, cómo deben ser estos utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo el nivel de clasificación de la información que a cada activo debe dársele. 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 y cuyo objetivo para este documento es dar cumplimiento a los siguientes tres puntos principales:[24]

- Inventario de activos: todos los activos deben estar claramente identificados donde Grow Data debe elaborar y mantener un inventario de estos.
- 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.

Teniendo en cuenta la norma descrita anteriormente, el inventario de activos de información que apalanca el servicio TI “Control de acceso” describe para cada activo la siguiente información:

- Información básica del activo (Identificador, nombre del activo, cantidad, descripción, Tipo de Activo).
- El nivel de clasificación de la información en cuanto a la confidencialidad, integridad y disponibilidad.

4.4 NORMA ISO 31000:2018 – GESTIÓN DEL RIESGO

La norma internacional ISO 31000:2018 es desarrollada y publicada por la Organización Internacional de Estandarización (ISO) la cual brinda los principios y

[24] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de Activos de Información. Bogotá: Mintic, 2020.

las directrices sobre la gestión del riesgo en las empresas u organizaciones. La versión de la norma ISO 31000 más reciente fue publicada en marzo del año 2018. En esta última versión de 2018 brinda recomendaciones orientadas a la gestión del riesgo permitiendo una mejor alineación con otras normas ISO como son la norma 9001:2015 o la norma 14001:2015.

Otro aspecto para tener en cuenta en la versión del 2018 es la importancia que se da a la alta dirección como principal actor para el cambio organizacional, de tal manera que este sea quien lidere el proceso de implementación para la gestión del riesgo en toda la organización.

El estándar ISO 31000:2018 es una norma que establece la importancia de la gestión del riesgo como una actividad intrínseca de cada organización y para que tenga éxito debe desarrollarse dentro de un contexto de liderazgo que incluya la cultura empresarial, la integración con los procesos y la inclusión de los empleados. Lo anterior genera un marco de referencia importante que permitirá no solo mitigar los riesgos, sino gestionar de manera más eficiente cualquier organización.[25]

Siguiendo las recomendaciones de la norma, se establecen las siguientes etapas de la gestión del riesgo para el servicio TI “Control de acceso”:

- Identificación del Riesgo, donde en conjunto con la organización, se inventariaron los riesgos a los que estaban expuestos los activos previamente documentados.
- Análisis del Riesgo, donde se establecen las métricas de probabilidad e impacto asociando las diferentes amenazas que pueden llegar a afectar los activos de información.
- Valoración del Riesgo, donde de acuerdo con las métricas de probabilidad e impacto se valoran los diferentes riesgos identificados, generando el correspondiente mapa de calor graficando los riesgos en las diferentes escalas de valoración.

Tratamiento del riesgo, donde se establecen las diferentes actividades o estrategias que se plantean para abordar de manera adecuada los riesgos, asignando a los responsables de la implementación de las actividades, el tiempo de implementación y los recursos necesarios requeridos.

[25] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).NTC-ISO:31000. Gestión del Riesgo. Principios y Directrices. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (INCONTEC), 2019.

4.5 MAGERIT – METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN V3

Esta metodología presenta un catálogo de amenazas posibles sobre los activos de un sistema de información. En resumen, la metodología de identificación de amenazas en MAGERIT versión 3 se basa en la identificación de los activos de información, la generación de una lista de posibles amenazas y la evaluación de riesgos para priorizar las medidas de seguridad que deben ser implementadas para mitigarlos. [26]Esta metodología es útil para ayudar a las organizaciones a identificar y abordar las amenazas a sus sistemas de información de manera sistemática y efectiva.

4.6 NORMA ISO/IEC 27001:2013 – ANEXO A

La norma internacional ISO/IEC 27001:2013 es desarrollada y publicada por la Organización Internacional de Estandarización (ISO) la cual suministra requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información. [27]La versión de la norma ISO/IEC 27001 utilizada para este proyecto es la del año 2013.

Esta norma permite a las organizaciones dar lineamientos para aplicar los controles necesarios para mitigar o eliminar el riesgo, es por eso por lo que para el servicio TI "Control de acceso" se acogió el anexo A el cual está dividido en 14 secciones, las cuales nos ayuda a servir de guía para la implementación de controles dirigidos a mejorar la seguridad de la información dentro del servicio TI, los cuales se listan a continuación:

- A.5 políticas de la seguridad de la información.
- A.6 organización de la seguridad de la información.
- A.7 seguridad de los recursos humanos.
- A.8 gestión de activos.
- A.9 control de acceso.
- A.10 criptografía.
- A.11 seguridad física y ambiental.
- A.12 seguridad de las operaciones.
- A.13 seguridad de las comunicaciones.
- A.14 adquisición, desarrollo y mantenimiento de sistemas.
- A.15 relaciones con los proveedores.

[26] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, 2012.

[27] INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27001. Anexo A Controles de Seguridad, 2013.

- A.16 gestión de incidentes de seguridad de la información
- A.17 aspectos de seguridad de la información de la gestión de continuidad de negocio.
- A.18 cumplimiento

De igual manera se utiliza el anexo 17 seguridad de la información en la gestión de continuidad del negocio en donde su objetivo es preservar la seguridad de la información, durante las fases de activación de desarrollos de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

De acuerdo con la norma se deben analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar, planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos, minimizando los efectos de las posibles interrupciones de las actividades normales de la organización, asociadas a desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos.

4.7 GUÍA PARA REALIZAR ANÁLISIS DE IMPACTO AL NEGOCIO - MINTIC

Mediante esta guía el Ministerio de Tecnologías de la Información y las Comunicaciones definen los lineamientos que las entidades u organizaciones públicas o privadas deben responder a una variedad de políticas de restablecimiento de actividades y servicios que apoyen el normal funcionamiento de las infraestructuras de TI y minimicen al máximo las interrupciones o fallas presentadas dentro de la organización.

Las organizaciones deben permanentemente monitorear y reconocer las amenazas más importantes de incidentes que afecten la normal operatividad de los servicios y los sistemas, de tal manera que se debe garantizar la continuidad del negocio a través de mecanismos de recuperación previamente probados y ajustados y que respondan en el menor tiempo posible a las soluciones de los problemas de interrupción generados.

El fin de la implementación del plan de continuidad de TI, es la protección y recuperación de los servicios críticos que se vean afectados por desastres naturales o interrupciones del servicio ocasionadas ya sea por los sistemas de información y comunicación o ya sean por el hombre en virtud de acciones involuntarias o para beneficio propio.
Así mismo, el análisis de impacto de negocio debe convertirse en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares de las organizaciones, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como

mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.

El análisis de impacto del negocio – BIA por sus siglas en inglés (Business Impact Analysis), está determinado por la construcción de un plan de continuidad del negocio para cada organización, que le permita a cada entidad continuar funcionando a pesar de un desastre ocurrido; el documento generado en este análisis deberá cumplir con lo expuesto en los requerimientos de la ISO/IEC 27001:2013 referente a los controles del anexo A, de este modo el documento BIA debe ser validado e implementado bajo las directrices de cada organización.

Se requieren planear las acciones necesarias durante el período en que la infraestructura de TI se encuentra inactiva y en proceso de recuperación y reanudación de los servicios para priorizar cuales actividades y servicios deben entrar en operación inmediatamente dentro de la entidad.

La fase de análisis de impacto del negocio – BIA, permite identificar con claridad los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

Cada organización debe disponer de un documento que permita identificar todas las áreas críticas del negocio y sea un instrumento para garantizar la medición de la magnitud del impacto operacional y financiero de la entidad, al momento de presentarse una interrupción. En esta etapa, el análisis de impacto del negocio debe poder clarificar los siguientes requerimientos:

- Identificar las funciones y procesos importantes para la supervivencia de la entidad al momento de la interrupción, esto es tener en cuenta cuales de los procesos son claves para que entren en operación rápidamente asignándoles la mayor prioridad posible, frente a los de menor prioridad; debe quedar claro que para los procesos identificados como no tan prioritarios se deben preparar también planes de recuperación.
- Revisar las consecuencias tanto operacionales como financieras, que una interrupción tendrá en los procesos considerados de alta prioridad.
- Estimar los tiempos de recuperación (RTO, RPO, MAO y MTD), en razón a las posibles alteraciones de los procesos considerados de alta prioridad para el funcionamiento de las infraestructuras de TI.[28]

[28] MINISTERIO DE LAS TECNOLOGÍAS Y LAS COMUNICACIONES - MinTic. Guía para realizar el Análisis de Impacto de Negocios BIA, 2015.

4.8 NORMA ISO 22301:2019

Se trata del primer estándar internacional para la gestión de la continuidad del Negocio (BCM), desarrollado para ayudar a las organizaciones a mitigar el riesgo del cese de un negocio o actividad ante las eventuales interrupciones.

El proceso de implementación inicia con la identificación de todos los elementos internos y externos con los que se relaciona la organización, continúa con la realización de los dos análisis claves: el análisis de impacto al negocio (BIA) y el análisis de riesgos de continuidad (RA), continúa con la definición de planes de respuesta y recuperación, que deberán asegurar que las estrategias son viables y operativas.[29]

[29] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019, International Organization for Standardization, 2019.

5. DISEÑO METODOLÓGICO

En este capítulo, se presenta una descripción detallada de la hipótesis y variables que se utilizaron en el anteproyecto para llevar a cabo la presente investigación; así mismo, las etapas que conforman toda la hoja de ruta que guía el desarrollo del documento. En resumen, este capítulo proporciona un marco detallado de cómo se llevó a cabo la investigación, para que otros investigadores puedan consultar los resultados obtenidos.

5.1 HIPÓTESIS

El diseño del Plan de Contingencia para el Servicio TI “Control de Acceso” ofrecido por Grow Data” ofrecerá una serie de actividades a realizar en caso de presentarse un incidente que afecte la operación.
El diseño del Plan de Contingencia para el Servicio TI “Control de Acceso” ofrecido por Grow Data” No ofrecerá una serie de actividades a realizar en caso de presentarse un incidente que afecte la operación.

5.2 VARIABLES

Variable independiente o explicativa. causa: Plan de Contingencia, Entidad, BIOSTAR 2
Variable dependiente. efecto: Incidentes, operación.

5.3 DESARROLLO DISEÑO METODOLÓGICO

El diseño metodológico desarrollado para este proyecto surge de la necesidad de abarcar la ejecución de cada una de las fases previas para el cumplimiento de los objetivos planteados anteriormente. En general la metodología consiste en la ejecución de las siguientes etapas y sus actividades, plasmadas en la figura 1 que se ilustra a continuación:

Figura 1. Fases diseño metodológico

Fuente: Elaboración propia

5.3.1 Etapa 1. planeación Esta etapa consiste en realizar la identificación del alcance del plan de contingencia, la información requerida y los objetivos del plan, así como también las expectativas de Grow data.

En esta fase se identifica la necesidad de validar con Grow Data la expectativa con respecto a lo que se requiere en el plan de contingencia, lo anterior permite tener mayor claridad sobre lo que se solicita y llevar a cabo el ejercicio de la forma esperada.

De igual forma, esta etapa permite determinar y planear la forma en que se desarrollará el plan de contingencia, para lo cual, se identificó que la forma más adecuada es desarrollar los diferentes formatos para el levantamiento de

información con respecto a los activos, riesgos de información y análisis de impacto al negocio.

También, dentro de esta etapa se definen las reuniones que se deben llevar a cabo en las etapas de levantamiento de información (Etapa 2, Etapa 3 y Etapa 5) con el fin de diligenciar de manera conjunta las plantillas que documentan la información de activos, riesgos de información y análisis de Impacto al negocio.

5.3.2 Etapa 2. levantamiento de información de activos Esta etapa consiste en realizar las actividades de levantamiento de activos de información, las cuales incluyen:

- Desarrollar la plantilla del levantamiento de información de los activos que apalancan el servicio TI “control de acceso”.
- Revisar y diligenciar el inventario de activos de información, los diagramas generales de la red actual, procedimientos, políticas, entre otros, teniendo en cuenta la valoración a nivel de confidencialidad, integridad y disponibilidad que tienen los activos de información para la organización.

5.3.3 Etapa 3. análisis de riesgos de información Esta fase consiste en realizar las actividades de levantamiento de riesgos de información, las cuales incluyen:

- Desarrollar y construir el análisis de riesgos de información de los activos que apalancan el servicio TI “control de acceso”.
- Establecer las métricas de probabilidad e impacto para el análisis de los riesgos identificados.
- Generar el mapa de calor de acuerdo con la valoración de los diferentes riesgos de información en cuanto a su probabilidad e impacto.

5.3.4 Etapa 4. definición de tratamiento de riesgos Esta etapa consiste en realizar las actividades para establecer las estrategias que se incluyen en el tratamiento de los riesgos identificados en la etapa anterior, las cuales incluyen:

- Definir el nivel de riesgo aceptable que presenten una valoración de 9 o superior.
- Identificar de acuerdo con las estrategias para el tratamiento de riesgos, los controles que se asocian a estas estrategias alineados con el anexo A de la norma ISO/IEC 27001:2013

5.3.5 Etapa 5. levantamiento de información BIA Esta etapa consiste en realizar las actividades de levantamiento del análisis de impacto al negocio sobre el servicio ti “control de acceso”, las cuales incluyen:

- Desarrollar el levantamiento de información del análisis de impacto al negocio.
- Revisar y diligenciar el análisis de impacto al negocio.

5.3.6 Etapa 6. fases de activación plan de contingencia Esta etapa consiste en realizar las actividades para el establecimiento de las etapas para la activación y vuelta a la normalidad del plan de contingencia, las cuales incluyen:

- Revisar y establecer los criterios que se deben tener en cuenta para entrar en contingencia.
- Revisar y establecer los criterios que se deben tener en cuenta para regresar a la operación normal después de salir de contingencia.
- Desarrollar y documentar el procedimiento con las actividades que se deben realizar antes, durante y después de la contingencia.

5.3.7 Etapa 7. definición de estrategias de continuidad Esta etapa consiste en realizar las actividades para la identificación de los escenarios de amenazas que pueden llegar a afectar la continuidad del servicio ti “control de acceso” y a la información generada de este, así mismo a la identificación de las estrategias que se desprenden de estos escenarios para asegurar la continuidad del servicio y de la información, las cuales incluyen:

- Revisar y establecer los múltiples escenarios de amenazas que pueden llegar a generar riesgos de continuidad sobre el servicio TI.
- Revisar y establecer las diferentes estrategias que la organización debe tener en cuenta para la mitigación de los escenarios de amenazas identificados previamente.

5.4 LEVANTAMIENTO DE INFORMACIÓN DE ACTIVOS

Se realiza el levantamiento de activos de información asociados al servicio TI "Control de Acceso" validando la criticidad respecto a su confidencialidad, integridad y disponibilidad e identificando el tipo y la descripción de este. Lo anterior de acuerdo con los controles del anexo A de la norma ISO/IEC 27001:2013 literal 8.1.1 Inventario de Activos. Para validar la criticidad de los activos de información de acuerdo con su confidencialidad se establece la siguiente escala de valoración de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MinTic la cual se plasma en el cuadro 1:

Cuadro 1. Escala valoración confidencialidad

Valoración	Calificación	Descripción
1	Alto (A) – Información pública reservada	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
2	Medio (M) – Información pública clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
3	Bajo (B) – Información pública	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a los procesos de la entidad.
4	(NC) – No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos INFORMACIÓN PUBLICA RESERVADA.
Fuente: Guía para la Gestión y Clasificación de Activos de Información - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia		

Para validar la criticidad de los activos de información de acuerdo con su integridad se establece la siguiente escala de valoración de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MinTic, la cual se plasma en el cuadro 2:

Cuadro 2. Escala valoración integridad

Valoración	Calificación	Descripción
1	Alto (A)	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 severas de la entidad.
2	Medio (M)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
3	Bajo (B)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
4	No Clasificada (NC)	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.
Fuente: Guía para la Gestión y Clasificación de Activos de Información - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia		

Para validar la criticidad de los activos de información de acuerdo con su disponibilidad se establece la siguiente escala de valoración de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MinTic, la cual se ilustra en el cuadro 3:

Cuadro 3. Escala valoración disponibilidad

Valoración	Calificación	Descripción
1	Alto (A)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externo.
2	Medio (M)	a no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad
3	Bajo (N)	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
4	No Clasificada (NC)	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA
Fuente: Guía para la Gestión y Clasificación de Activos de Información - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia		

En el cuadro 4, se describen los activos de información documentando los siguientes campos: Identificador, activo, cantidad, descripción, tipo de Activo, confidencialidad, integridad, disponibilidad.

Cuadro 4. Inventario de activos de información

Identificador	Activo	Cantidad	Descripción	Tipo de activo	Confidencialidad	Integridad	Disponibilidad
Hw-1	Biométrico	3	Comunicación TCP/IP, interfaz RS-485, con lector de huellas y tarjeta de proximidad.	Hardware	Bajo	Medio	Alto
Hw-2	Cámara Bala	1	Bala: 4 MP, Sensor de imagen: CMOS de escaneo progresivo de 1/3″, Día y noche: Filtro de corte IR con interruptor automático.	Hardware	Bajo	Medio	Alto
Hw-3	Cámara Domo	4	CMOS de escaneo progresivo de 1/1.8 pulgadas, sensor de imagen de 6 megapíxeles	Hardware	Bajo	Medio	Alto
Hw-4	Cámara Ojo de Pez	2	panorámica, 180/360 grados, con lente de 0.049 in, IR día/noche poe/12 VDC	Hardware	Bajo	Medio	Alto
Hw-5	Cámara PTZ	1	Detector de movimiento e infrarrojo.	Hardware	Bajo	Medio	Alto
Hw-6	NVR	2	Salida de video / audio, Salida HDMI / VGA: | 2 canales, resolución: HMDI1 / VGA1: HDMI1: 4K Interfaz de red: | 2 RJ-45 Entrada de video / audio	Hardware	Medio	Alto	Alto
Hw-7	Servidor de Aplicaciones	1	− OS Windows server 2008 R2 Estándar. − CPU 4 core. − Ram 16Gb HDD 3TB	Hardware	Medio	Alto	Alto
Hw-8	Molinete brazo bidireccional	2	− Sistema resortado. − Caja porta lectora: Opcional. Cuerpo: Acero Inoxidable.	Hardware	Bajo	Medio	Alto

Cuadro 4. (Continuación)

Identificador	Activo	Cantidad	Descripción	Tipo de activo	Confidencialidad	Integridad	Disponibilidad
Hw-9	Torniquete	1	- Acero Inoxidable - Pictogramas De Señalización De Entrada Y Salida.	Hardware	Bajo	Medio	Alto
Hw-10	Brazo	1	Apto para puerta simple con un ancho máximo de puerta.	Hardware	Bajo	Medio	Alto
Hw-11	Electroimán	1	Con mecanismos de apertura PULSADOR, BIOMETRICO, LECTOR PROXIMIDAD instalación sobrepuesta.	Hardware	Bajo	Medio	Alto
Hw-12	Tarjetas de Proximidad	100	Frecuencia de 125khz	Hardware	Bajo	Medio	Alto
Hw-13	Sensores de Movimiento	20	Tipo de fuente led, con una capacidad de foco.	Hardware	Bajo	Medio	Alto
HW-14	Sensores Magnéticos	20	Potencia: 3 Vatios Máxima distancia de trabajo: 25 metros	Hardware	Bajo	Medio	Alto
Hw-15	Controlador PTZ	1	Controlador para el reconocimiento manipulación de las cámaras PTZ	Software	Medio	Medio	Alto
Hw-16	NAS	1	NAS Hikvision almacenamiento grabación.	Hardware	Alto	Medio	Alto
Hw-17	Router	1	Dispositivo que conecta la red interna con el proveedor de servicios de Internet,	Hardware	Medio	Bajo	Alto
Hw-18	Switch	2	Dispositivo de interconexión que conecta los servidores y los equipos de lectura biométrica.	Hardware	Medio	Bajo	Alto

Cuadro 4. (Continuación)

Identificador	Activo	Cantidad	Descripción	Tipo de activo	Confidencialidad	Integridad	Disponibilidad
Sw-1	BIOStar 2	1	Software que administra: - Control de acceso - Usuarios - Monitoreo de cámaras Para sistema operativo Windows y con base de datos MariaDB.	Software	Alto	Alto	Alto
Sw-2	BMS ARQUERO	1	Software integrador de CCTV y control biométrico.	Software	Alto	Medio	Alto
Rh-1	Líder del Servicio	1	Gerente del proyecto encargado del servicio TI “Control de Acceso”	Recurso Humano	Bajo	Medio	Alto
Rh-2	Administrador BIOStar 2	1	Ingeniero de sistemas con experiencia en administración de sistemas de información y bases de datos	Recurso Humano	Bajo	Medio	Alto
Rh-3	Administrador ARQUERO	1	Ingeniero de sistemas con experiencia en administración de sistemas de información y auditoria de sistemas	Recurso Humano	Bajo	Medio	Alto
Rh-4	Administrador de Hardware	1	Ingeniero de sistemas con experiencia en administración de infraestructura de TI	Recurso Humano	Bajo	Medio	Alto
Rh-5	Administrador de NAS	1	Ingeniero de sistemas con experiencia en administración de infraestructura de almacenamiento	Recurso Humano	Bajo	Medio	Alto
Rh-6	Administrador de Circuito Cerrado de Televisión	1	Ingeniero de Telecomunicaciones con experiencia en el manejo de circuito cerrado de televisión	Recurso Humano	Bajo	Medio	Alto

Fuente: Elaboración propia

5.5 ANÁLISIS DE RIESGOS DE INFORMACIÓN

Se realiza el análisis de riesgos de los activos de información asociados al servicio TI "Control de Acceso", identificando los riesgos a los cuales se pueden ver afectados estos activos provocando impactos en la prestación del servicio, asociándolos con su respectivas amenazas, probabilidad e impacto existentes sobre estos.

Lo anterior de acuerdo con las buenas prácticas de la norma ISO 31000:2018 en el numeral 6.4 Evaluación del riesgo. Para un mejor entendimiento de los riesgos analizados, en el cuadro 5 se establecen los valores de probabilidad establecidos para el presente análisis.

Cuadro 5. Valoración probabilidad

Probabilidad	Valoración
Rara vez No se ha presentado en los últimos 5 años	1
Improbable Al menos una vez en los últimos 5 años	2
Posible Al menos una vez en los últimos 2 años	3
Probable Al menos una vez en el último año	4
Casi Seguro Más de una vez al año	5
Fuente: Elaboración propia	

De igual manera en el cuadro 6 se establecen los valores de impacto establecidos para el presente análisis.

Cuadro 6. Valoración de impacto

Impacto	Valoración
Insignificante Un valor mayor o igual 0,5% de la ejecución presupuestal	1
Menor Un valor mayor o igual 1% de la ejecución presupuestal	2
Moderado Un valor mayor o igual 5% de la ejecución presupuestal	3
Mayor Un valor mayor o igual 20% de la ejecución presupuestal	4

Cuadro 6. (Continuación)

Impacto	Valoración
Catastrófico Un valor mayor o igual 50% de la ejecución presupuestal	5

Fuente: Elaboración propia

En el cuadro 7 se enlistan las amenazas documentadas en el catálogo que entrega Magerit en su versión 3.0, de las cuales se identificarán aquellas que presentan mayor prioridad para Grow Data.

Cuadro 7. Lista de amenazas identificadas

Identificador de Amenaza	Descripción
A01	Acceso no autorizado
A02	Negación de las acciones realizadas
A03	Interceptación no autorizada
A04	Alteración o modificación no autorizadas
A05	Destrucción o eliminación no autorizada
A06	Divulgación no autorizada
A07	Sabotaje (daño intencional)
A08	Hurto, Robo o Pérdida
A09	Acto de vandalismo o ataque destructivo
A10	Abuso en los privilegios de acceso
A11	Daño por fuego, agua, polvo, vibraciones o suciedad
A12	Uso no previsto o inadecuado
A13	Daño por condiciones ambientales inadecuadas
A14	Error en el uso
A15	Engaño o manipulación (Ingeniería social)
A16	Fuga o interceptación
A17	Error por mantenimiento o actualización
A18	Agotamiento de recursos o capacidades
A19	Degradación o deterioro
A20	Alteración de funcionalidades
A21	Infección por software dañino o malicioso
A22	Falla o mal funcionamiento
A23	Falla o Error en la instalación, administración o custodia
A24	Denegación de acceso o inaccesibilidad
A25	Comportamiento inesperado o anormal
A26	Ocupación no autorizada o invasión de espacio
A27	Cambio o ajuste no controlado
A28	Redireccionamiento no autorizado
A29	Error o falla en el monitoreo
A30	Extorsión o amenazas
A31	Desastres naturales

Cuadro 7. (Continuación)

Identificador de Amenaza	Descripción
A32	Suplantación de la identidad
A33	Corte del suministro eléctrico
A34	Interrupción de suministros esenciales
A35	Daño o destrucción no intencional
A36	Ausencia de personal
Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	

En el cuadro 8 se visualizan las amenazas que Grow Data prioriza en su identificación sobre el servicio TI “Control de Acceso”.

Cuadro 8. Lista de amenazas priorizadas por Grow Data

Identificador de Amenaza	Descripción
A07	Sabotaje (daño intencional)
A22	Infección por software dañino o malicioso
A33	Corte del suministro eléctrico
A17	Error por mantenimiento o actualización
A36	Ausencia de personal
A02	Negación de las acciones realizadas
A32	Suplantación de la identidad
Fuente: MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.	

Los resultados del análisis de los riesgos de información identificados en la matriz se describen en el cuadro 9:

Cuadro 9. Análisis de riesgos de información inherentes

Activo	Amenaza	Probabilidad	Impacto	Valoración Riesgo	ID Riesgo
Hw-1	A07	3	3	9	R1
	A22	4	5	20	R2
	A33	3	3	9	R3
Hw-2	A22	4	4	16	R4
	A07	3	3	9	R5
	A33	3	3	9	R6
Hw-3	A07	3	3	9	R7
	A22	3	3	9	R8
	A33	3	3	9	R9
Hw-4	A07	3	3	9	R10
	A22	3	3	9	R11
	A33	3	3	9	R12

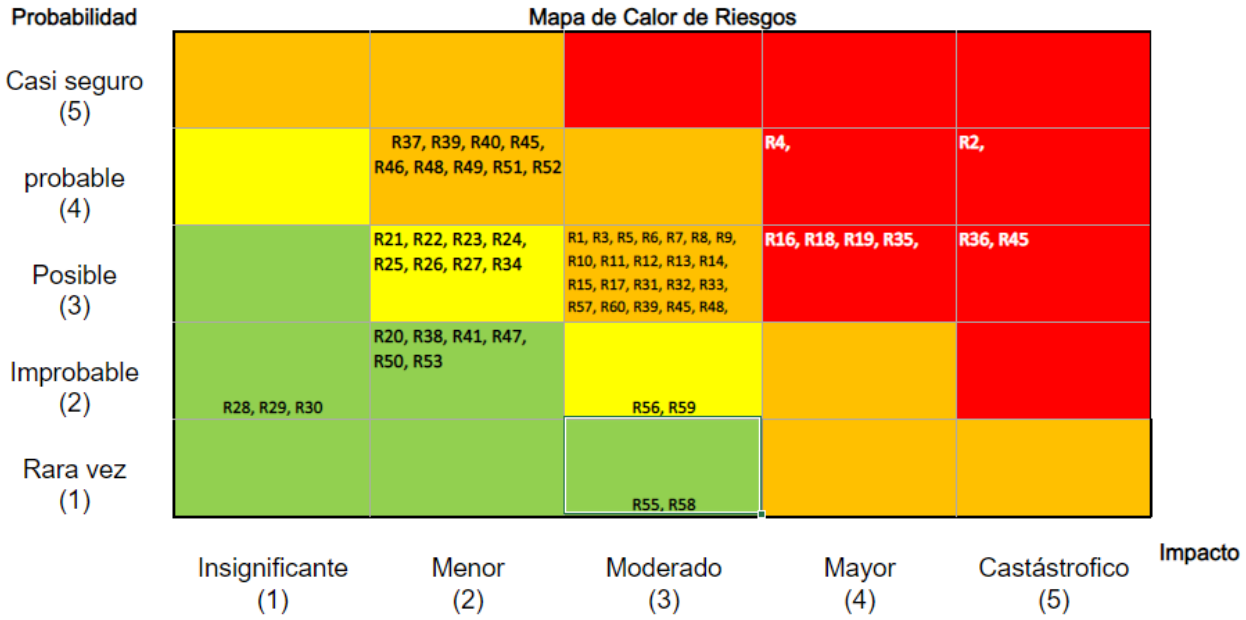
Cuadro 9. (Continuación)

Activo	Amenaza	Probabilidad	Impacto	Valoración Riesgo	ID Riesgo
Hw-5	A07	3	3	9	R13
	A22	3	3	9	R14
	A33	3	3	9	R15
Hw-6	A22	3	4	12	R16
	A33	3	3	9	R17
Hw-7	A17	3	4	12	R18
	A22	3	4	12	R19
Hw-8	A07	2	2	4	R20
	A17	3	2	6	R21
Hw-9	A22	3	2	6	R22
	A07	3	2	6	R23
	A17	3	2	6	R24
Hw-10	A22	3	2	6	R25
	A07	3	2	6	R26
	A17	3	2	6	R27
Hw-11	A22	2	1	2	R28
	A07	2	1	2	R29
Hw-12	A17	2	1	2	R30
	A22	3	3	9	R31
	A07	3	3	9	R32
	A17	3	3	9	R33
Hw-13	A17	3	2	6	R34
	A22	3	4	12	R35
Hw-17	A07	1	3	3	R55
	A22	2	3	6	R56
	A33	3	3	9	R57
Hw-18	A07	1	3	3	R58
	A22	2	3	6	R59
	A33	3	3	9	R60
Sw-1	A17	3	5	15	R36
Sw-2	A32	3	5	15	R45
Rh-1	A36	4	2	8	R37
	A02	2	2	4	R38
	A32	3	3	9	R39
Rh-2	A36	4	2	8	R40
	A02	2	2	4	R41
	A32	3	3	9	R45
Rh-4	A36	4	2	8	R46
	A02	2	2	4	R47
	A32	3	3	9	R48
Rh-5	A36	4	2	8	R49
	A02	2	2	4	R50
	A32	3	3	9	R51
Rh-6	A36	4	2	8	R52
	A02	2	2	4	R53
	A32	3	3	9	R54

Fuente: Elaboración propia

En la figura 2 se encuentra el mapa de calor resultado de los riesgos analizados después de valorarlos en su impacto y probabilidad de acuerdo con las escalas de valoración documentadas previamente, De esta manera, es posible visualizar de manera clara y concisa los riesgos que presentan una mayor prioridad para su tratamiento sobre el servicio TI “Control de Acceso”:

Figura 2. Mapa de Calor de Riesgos Inherentes



Fuente: Elaboración propia

5.6 TRATAMIENTO DE RIESGOS

El presente ítem contiene las actividades requeridas para mitigar los riesgos asociados al servicio TI “Control de acceso” igual o superior a 9 en la valoración de riesgo de acuerdo con el nivel de riesgo aceptado y especificado por Grow Data.

En el cuadro 10 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por mal funcionamiento del activo de información tipo Biométrico.

Cuadro 10. Pérdida de disponibilidad por mal funcionamiento del Biométrico

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R2
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos. A.11.1.4 Protección contra amenazas externas y ambientales

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de los biométricos con el fin de contar con la información actualizada de estos.
2	Fortalecer los planes de mantenimiento preventivos y correctivos sobre los biométricos realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales, teniendo en cuenta las partes del biométrico que presentan mayor desgaste por su uso las cuales son: cubierta, ventana, cable de datos y conector USB.
3	Desarrollar y socializar un manual de buen uso de las partes (cubierta, ventana, cable de datos y conector USB) que conforman los biométricos por parte de los funcionarios.
4	Fortalecer los planes de actualización tecnológica de los biométricos realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Implementar un sistema de monitoreo y supervisión para detectar problemas con el sistema biométrico y tomar medidas para solucionarlos de manera oportuna.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 11 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por errores en la actualización del sistema Biostar2.

Cuadro 11. Pérdida de disponibilidad por error en actualizaciones al sistema Biostar2

Nombre del Tratamiento	Fortalecimiento de procedimientos de actualizaciones de software
Descripción del tratamiento	Mejora en los planes de actualizaciones de sistema operativo, parches de seguridad, etc.
Riesgo Asociado	R36
Controles Asociados	A.12.3.1 Respaldo de la información A.12.5.1 Instalación de software en sistemas operativos A.12.6.2 Restricción sobre la instalación de software A.12.1.2 Gestión de Cambios
Estrategias por Realizar	
Estrategia	Descripción
1	Implementación de procedimientos de réplica de información del sistema Biostar2 en un ambiente secundario y protegido.
2	Desarrollar procedimientos de actualización del sistema Biostar2 de manera segura en ambiente secundario.
3	Desarrollar procedimientos de instalación y actualización del sistema operativo que aloje el aplicativo Biostar2.
4	Establecer los roles autorizados para la instalación y/o actualización de sistema Biostar2 referente al servicio TI "control de acceso".
5	Cifrar la información almacenada en el sistema Biostar2 de acuerdo con su clasificación.
6	Verificación de los programas de seguridad especifica como herramientas para virus, versiones de software, reparaciones y arreglos de software.
7	Asegurar el uso de software licenciado del sistema Biostar2 usado por Grow data para la prestación del servicio TI.
8	Registrar las acciones a realizar en el proceso de actualización del aplicativo, como también las acciones a reversar los cambios efectuados por mal funcionamiento.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación, formato de gestión de cambios.
Fuente: Elaboración propia	

En el cuadro 12 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por el mal funcionamiento de los activos tipo cámara bala.

Cuadro 12. Pérdida de disponibilidad por mal funcionamiento de la cámara Bala

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R4
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.11.2.3 Seguridad en el cableado
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de la cámara Bala con el fin de contar con la información actualizada de estas.
2	Fortalecer los planes de mantenimiento preventivos y correctivos sobre la cámara Bala realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales, teniendo en cuenta las partes de la cámara bala que presentan mayor susceptibilidad por su uso, las cuales son: óptica, led y sensor.
3	Desarrollar y socializar un manual de buen uso de las partes (óptica, led y sensor) que conforman la cámara Bala por parte de los funcionarios.
4	Fortalecer los planes de actualización tecnológica de la cámara Bala realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Implementar técnicas de cableado estructurado para garantizar una organización y topología sólida.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 13 se documentan las seis estrategias y los seis controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por el mal funcionamiento de los activos tipo NVR.

Cuadro 13. Pérdida de disponibilidad por mal funcionamiento del NVR

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R16
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.9.4.4 Uso de programas utilitarios privilegiados A.11.2.4 Mantenimiento de equipos A.10.1.1 Política controles criptográficos

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario del NVR con el fin de contar con la información actualizada de estos.
2	Fortalecer los planes de mantenimiento preventivos y correctivos sobre el NVR realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales, teniendo en cuenta las partes del NVR que pueden presentan mayor susceptibilidad por su uso, las cuales son: cubiertas, panel frontal, puertos USB, panel RJ45, puerto LAN, puerto de video, conector de alimentación, tarjeta RAM, disco duro, tarjeta de red, procesador.
3	Desarrollar y socializar un manual de buen uso de las partes (cubiertas, panel frontal, puertos USB, panel RJ45, puerto LAN, puerto de video, conector de alimentación, tarjeta RAM, disco duro, tarjeta de red, procesador) que conforman el NVR por parte de los funcionarios.
4	Crear y gestionar usuario con privilegios de instalación de programas confiables para el NVR
5	Fortalecer los planes de actualización tecnológica del NVR realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
6	Desarrollar una política de control criptográfico sobre las imágenes o videos almacenados en el NVR.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data

Fuente: Elaboración propia

En el cuadro 14 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por errores en actualizaciones sobre el servidor de aplicaciones.

Cuadro 14. Pérdida de disponibilidad por error en actualizaciones al servidor de aplicaciones

Nombre del Tratamiento	Fortalecimiento de procedimientos de actualizaciones de software
Descripción del tratamiento	Mejora en los planes de actualizaciones de sistema operativo, parches de seguridad, etc.
Riesgo Asociado	R18
Controles Asociados	A.12.3.1 Respaldo de la información A.12.5.1 Instalación de software en sistemas operativos A.12.6.2 Restricción sobre la instalación de software A.9.4.1 Restricción del acceso a la información
Estrategias por Realizar	
Estrategia	Descripción
1	Implementación de procedimientos de réplica de la información del servidor de aplicaciones en un ambiente secundario y protegido.
2	Generar un ítem en el procedimiento de la réplica de información donde se identifique la generación de un punto de restauración antes de la actualización del servidor de aplicaciones.
3	Desarrollar procedimientos de actualización del servidor de aplicaciones de manera segura en ambiente secundario.
4	Desarrollar procedimientos de instalación y actualización del sistema operativo del servidor de aplicaciones.
5	Establecer los roles autorizados para la instalación y/o actualización de servidor de aplicaciones referente al servicio TI "control de acceso".
6	Realizar o establecer accesos físicos o lógicos para protección del servidor de aplicaciones valorado como un activo altamente clasificado.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación
Fuente: Elaboración propia	

En el cuadro 15 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por mal funcionamiento del servidor de aplicaciones.

Cuadro 15. Pérdida de disponibilidad por mal funcionamiento servidor de aplicaciones

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R19
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.12.3.1 Copias Seguridad de Información

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario del servidor de aplicaciones con el fin de contar con la información actualizada de estos.
2	Desarrollar y socializar un manual de buen uso de las partes (tarjeta de red, tarjeta de video, conector de alimentación, memoria RAM, disco duro, procesador, board) que conforman el servidor de aplicaciones por parte de los funcionarios.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre el servidor de aplicaciones realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales, teniendo en cuenta las partes del servidor de aplicaciones que pueden presentan mayor susceptibilidad por su uso, las cuales son: tarjeta de red, tarjeta de video, conector de alimentación, memoria RAM, disco duro, procesador, board.
4	Fortalecer los planes de actualización tecnológica del servidor de aplicaciones realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Desarrollar una política de copias de seguridad especificando periodicidad, necesidad de respaldo de información como son software, aplicación y datos de configuración de la aplicación.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 16 se documentan las seis estrategias y los seis controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por errores al momento de realizar el mantenimiento a la NAS.

Cuadro 16. Pérdida de disponibilidad por errores en mantenimientos de la NAS

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R35
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.12.3.1 Copias de respaldo de la información A.12.6.2 Restricciones en la instalación de software

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de la NAS con el fin de contar con la información actualizada de estos.
2	Fortalecer los planes de mantenimiento preventivos y correctivos sobre la NAS realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales, teniendo en cuenta las partes de la NAS que pueden presentan mayor susceptibilidad por su uso, las cuales son: frontal, bahías, puerto USB, procesador, memoria RAM, módulos MSATA, memoria caché, interfaces de discos duros, ventilación, interfaces de red.
3	Fortalecer los planes de actualización tecnológica de la NAS realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Desarrollar y socializar un manual de buen uso de las partes (frontal, bahías, puerto USB, procesador, memoria RAM, módulos MSATA, memoria caché, interfaces de discos duros, ventilación, interfaces de red) que conforman la NAS por parte de los funcionarios.
5	Desarrollar un procedimiento que indique que es de obligatorio cumplimiento la generación de copias de respaldo en el momento de realizar un mantenimiento sobre la NAS.
6	Desarrollar una de mantenimiento e instalación de software donde se especifique la idoneidad del personal que realiza mantenimiento y actualizaciones a la NAS.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 17 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos tipo Biométricos de manera intencional.

Cuadro 17. Pérdida de disponibilidad por daño intencional sobre el Biométrico

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R1
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.12.6.1 Gestión de vulnerabilidades técnicas
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de los biométricos donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar los biométricos afectados por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre los biométricos.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por el biométrico.
5	Intervenir los biométricos que han sido atacados o comprometidos bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de los biométricos afectados tras la materialización del daño intencional generando la indisponibilidad y no operación de estos.
7	Mantener actualizados la información de los contratos de los proveedores y/o fabricantes de los biométricos.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 18 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo Biométrico.

Cuadro 18. Pérdida de disponibilidad del Biométrico por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R3
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.11.1.4 Protección contra amenazas externas y del ambiente
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico de los biométricos en caso de ser requerido.
2	Instalación de las UPS al servicio de los biométricos previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan el biométrico realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Desarrollar planes de continuidad donde se especifiquen estrategias de redundancia para el fluido eléctrico.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación, Planes de Continuidad Equipos: UPS
Fuente: Elaboración propia	

En el cuadro 19 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos tipo cámara bala de manera intencional.

Cuadro 19. Pérdida de disponibilidad por daño intencional sobre la cámara Bala

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R5
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.12.4.1 Registro de Eventos
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de la cámara Bala donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar la cámara Bala afectadas por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre la cámara Bala.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por la cámara bala.
5	Intervenir las cámaras bala que han sido atacadas o comprometidas bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de las cámaras balas afectadas tras la materialización del daño intencional generando la indisponibilidad y no operación de estas.
7	Implementar un registro de eventos de fallas en la operación y/o desconexión de la cámara bala.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 20 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo cámara bala.

Cuadro 20. Pérdida de disponibilidad de cámara Bala por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R6
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.17.1.3 Verificar, Revisar y evaluar la continuidad de la seguridad de la información
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico de las cámaras balas en caso de ser requerido.
2	Instalación de las UPS al servicio de las cámaras balas previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan las cámaras balas realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Realizar una lista de chequeo para evaluar la disponibilidad de la cámara bala por ausencia del fluido eléctrico.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS
Fuente: Elaboración propia	

En el cuadro 21 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos tipo cámara domo de manera intencional.

Cuadro 21. Pérdida de disponibilidad por daño intencional sobre la cámara Domo

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R7
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de la cámara domo donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar la cámara domo afectadas por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre la cámara domo.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por la cámara domo.
5	Intervenir las cámaras domo que han sido atacadas o comprometidas bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de las cámaras domo afectadas tras la materialización del daño intencional generando la indisponibilidad y no operación de estas.
7	Hacer valer la normatividad por cualquier daño o perjuicio intencional realizado sobre la cámara domo.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 22 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por el mal funcionamiento de los activos de información tipo cámara domo.

Cuadro 22. Pérdida de disponibilidad por mal funcionamiento cámara Domo

Nombre del Tratamiento		Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento		Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado		R8
Controles Asociados		A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.16.1.6 Aprendiendo de los incidentes de seguridad de la información
Estrategias por Realizar		
Estrategia	Descripción	
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de las cámaras domo con el fin de contar con la información actualizada de estos.	
2	Desarrollar y socializar un manual de buen uso de las cámaras domo por parte de los funcionarios.	
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las cámaras domo realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.	
4	Fortalecer los planes de actualización tecnológica de las cámaras domo realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.	
5	Establecer una base de datos de incidentes presentados por mal funcionamiento cámara domo para futuras soluciones.	
Duración estimada del tratamiento del riesgo		1 año
Recursos necesarios para el tratamiento del riesgo		Personas: funcionarios Grow Data
Fuente: Elaboración propia		

En el cuadro 23 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo cámara domo.

Cuadro 23. Pérdida de disponibilidad de cámaras Domo por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R9
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.18.2.2 Cumplimiento de la política y las normas de seguridad
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico de las cámaras domo en caso de ser requerido.
2	Instalación de las UPS al servicio de las cámaras domo previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan las cámaras domo realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Establecer normas mínimas de la instalación del fluido eléctrico para la cámara domo.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS
Fuente: Elaboración propia	

En el cuadro 24 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos tipo cámara ojo de pez de manera intencional.

Cuadro 24. Pérdida de disponibilidad por daño intencional sobre cámara ojo de pez

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R10
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.8.1.3 Uso aceptable de los activos
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de las cámaras ojo de pez donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar las cámaras ojo de pez afectados por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre las cámaras ojo de pez.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por la cámara ojo de pez.
5	Intervenir las cámaras ojo de pez que han sido atacadas o comprometidas bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de las cámaras ojo de pez afectadas tras la materialización del daño intencional generando la indisponibilidad y no operación de estas.
7	Creación de política para la administración y uso correcto de las cámaras ojos de pez.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 25 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por el mal funcionamiento de los activos de información tipo cámara ojo de pez.

Cuadro 25. Pérdida de disponibilidad por mal funcionamiento cámara ojo de pez

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R11
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.18.2.2 Cumplimiento de la política y las normas de seguridad

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de las cámaras ojo de pez con el fin de contar con la información actualizada de estos.
2	Desarrollar y socializar un manual de buen uso de las cámaras ojo de pez servidor de aplicaciones por parte de los funcionarios.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las cámaras ojo de pez realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Fortalecer los planes de actualización tecnológica de las cámaras ojo de pez realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Establecimiento de política donde se establezca la identificación los fallos en las actualizaciones y las medidas correctivas.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data

Fuente: Elaboración propia

En el cuadro 26 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo cámara ojo de pez.

Cuadro 26. Pérdida de disponibilidad de cámaras ojo de pez por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R12
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.15.1.2 Seguridad en los acuerdos con proveedores
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico de las cámaras ojo de pez en caso de ser requerido.
2	Instalación de las UPS al servicio de las cámaras ojo de pez previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan las cámaras ojo de pez realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Generar clausulas en los contratos del proveedor para garantizar la no ausencia del fluido eléctrico en las cámaras ojo de pez.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS
Fuente: Elaboración propia	

En el cuadro 27 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos de información tipo cámara PTZ de manera intencional

Cuadro 27. Pérdida de disponibilidad por daño intencional sobre cámara PTZ

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R13
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.16.1.1 Responsabilidades y procedimientos
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de las cámaras PTZ donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar las cámaras PTZ afectados por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre las cámaras PTZ.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por la cámara PTZ.
5	Intervenir las cámaras PTZ que han sido atacadas o comprometidas bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de las cámaras PTZ afectadas tras la materialización del daño intencional generando la indisponibilidad y no operación de estas.
7	Asignar un responsable para la gestión del incidente que genere perdida de disponibilidad de la cámara PTZ.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 28 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por el mal funcionamiento de los activos de información tipo cámara PTZ.

Cuadro 28. Pérdida de disponibilidad por mal funcionamiento cámara PTZ

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R14
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.16.1.7 Recolección de evidencia

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de las cámaras PTZ con el fin de contar con la información actualizada de estos.
2	Desarrollar y socializar un manual de buen uso de las cámaras PTZ por parte de los funcionarios.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las cámaras PTZ realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Fortalecer los planes de actualización tecnológica de las cámaras PTZ realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Establecer un protocolo de recopilación de estados de las cámaras PTZ que ayude en la recolección de evidencia en caso de presentarse un incidente.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data

Fuente: Elaboración propia

En el cuadro 29 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo cámara PTZ.

Cuadro 29. Pérdida de disponibilidad de cámaras PTZ por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R15
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.12.6.1 Gestión de Vulnerabilidades técnicas

Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico de las cámaras PTZ en caso de ser requerido.
2	Instalación de las UPS al servicio de las cámaras PTZ previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan las cámaras PTZ realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Documentar las vulnerabilidades a nivel técnico de las UPS relacionadas a las cámaras PTZ.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS

Fuente: Elaboración propia

En el cuadro 30 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por el mal funcionamiento de los activos de información tipo NVR.

Cuadro 30. Pérdida de disponibilidad por mal funcionamiento NVR

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R16
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario del NVR con el fin de contar con la información actualizada de estos.
2	Desarrollar y socializar un manual de buen uso del NVR por parte de los funcionarios.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre el NVR realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Fortalecer los planes de actualización tecnológica del NVR realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Establecer criterios de priorización alta para los incidentes que se materializan afectando la continuidad del NVR.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 31 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo NVR

Cuadro 31. Pérdida de disponibilidad del NVR por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R17
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.17.1.1 Planificación de la continuidad de la seguridad de la información

Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico del NVR en caso de ser requerido.
2	Instalación de las UPS al servicio del NVR previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan el NVR realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Documentar un plan de continuidad que establezca la redundancia del fluido eléctrico para el NRV.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS

Fuente: Elaboración propia

En el cuadro 32 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por el mal funcionamiento de los activos de información tipo sensor.

Cuadro 32. Pérdida de disponibilidad por mal funcionamiento sensor

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R31
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.15.1.3 Cadena de suministro de tecnologías de la información y las comunicaciones

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de los sensores con el fin de contar con la información actualizada de estos.
2	Desarrollar y socializar un manual de buen uso de los sensores por parte de los funcionarios.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre los sensores realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Fortalecer los planes de actualización tecnológica de los sensores realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
5	Exigir al proveedor que los subcontratistas tengan clausulas para la aplicación de la seguridad en el suministro de los sensores.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data

Fuente: Elaboración propia

En el cuadro 33 se documentan las cinco estrategias y los cinco controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad por errores al momento de realizar el mantenimiento a los sensores.

Cuadro 33. Pérdida de disponibilidad por errores en mantenimientos del sensor

Nombre del Tratamiento	Fortalecimiento de los planes de mantenimiento y renovación de los activos de información.
Descripción del tratamiento	Mejora en los tiempos de mantenimiento y de renovación sobre el activo de información.
Riesgo Asociado	R33
Controles Asociados	A.8.1.1 Inventario de Activos A.8.1.2 Propiedad de los Activos A.8.1.3 Uso aceptable de los activos A.11.2.4 Mantenimiento de equipos A.12.1.1 Procedimientos documentados de operación
Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en el registro del inventario de los sensores con el fin de contar con la información actualizada de estos.
2	Fortalecer los planes de mantenimiento preventivos y correctivos sobre los sensores realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
3	Fortalecer los planes de actualización tecnológica de los sensores realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Desarrollar y socializar un manual de buen uso de los sensores por parte de los funcionarios.
5	Documentar los mantenimientos requeridos por el tipo de sensor.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 34 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por daños realizados sobre los activos de información tipo sensor de manera intencional.

Cuadro 34. Pérdida de disponibilidad por daño intencional sobre sensor

Nombre del Tratamiento	Fortalecimiento de la custodia del activo de información de cara al público.
Descripción del tratamiento	Mejora en el cuidado y la vigilancia que el personal de la entidad debe ejercer sobre el activo de información.
Riesgo Asociado	R32
Controles Asociados	A.11.1.4 Protección contra amenazas externas y ambientales. A.11.2.1 Ubicación y protección de los equipos. A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones A.16.1.3 Reporte de debilidades de seguridad de la información

Estrategias por Realizar	
Estrategia	Descripción
1	Desarrollar un procedimiento de fortalecimiento en la custodia de sensores donde se pueden tener acceso físico a estos.
2	Implementación de un ambiente secundario en donde se cuente con la capacidad de recuperar los sensores afectados por el daño intencional.
3	Desarrollar y socializar políticas de seguridad física sobre los sensores.
4	Implementación de medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida por el sensor.
5	Intervenir los sensores que han sido atacados o comprometidos bajo los lineamientos establecidos garantizando respuesta rápida, eficaz y ordenada.
6	Valoración de los sensores afectados tras la materialización del daño intencional generando la indisponibilidad y no operación de estos.
7	Creación de reporte donde se identifique las posibles debilidades para la perdida de disponibilidad por daño intencional sobre el sensor.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data
Fuente: Elaboración propia	

En el cuadro 35 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia del administrador de la plataforma Biostar2.

Cuadro 35. Pérdida de disponibilidad por ausencia del administrador Biostar2

Nombre del Tratamiento	Fortalecimiento en la asignación de personal de respaldo
Descripción del tratamiento	Asignación y nombramiento de personal que asuma los roles clave que presenten ausencia
Riesgo Asociado	R40
Controles Asociados	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.1.2 Términos y condiciones del empleo A.6.1.2 Segregación de funciones
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas de respaldo del administrador de Biostar2 para la prestación del servicio TI “control de acceso.”
2	Crear mecanismos de obligatoriedad en la asistencia a las capacitaciones referentes a la seguridad de la información por parte del rol administrador de Biostar2.
3	Crear mecanismos contractuales para el rol administrador Biostar2 para el cumplimiento de las funciones referentes a la seguridad.
4	Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían respaldar en caso de que el administrador de Biostar2 no pueda ejercer sus responsabilidades, afectando la continuidad del servicio TI.
5	Activar a aquellos colaboradores que sean respaldo del administrador de Biostar2, en caso de que este no pueda ejercer sus responsabilidades.
6	Preparación de la ausencia prolongada del administrador de Biostar2 por enfermedad personal y/o familiar, por aplicación de medidas de protección como el aislamiento obligatorio o por la interrupción o disminución del transporte público.
7	Habilitar procedimientos que permitan que el administrador de Biostar2 pueda realizar sus actividades por medio del teletrabajo, con horario flexible o con alternancia.
8	Asignación funciones a otros perfiles mientras el administrador del aplicativo Biostar2 se encuentre ausente.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Contratos laborales
Fuente: Elaboración propia	

En el cuadro 36 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la negación sobre las acciones y funciones del administrador de la plataforma Biostar2.

Cuadro 36. Pérdida de disponibilidad por negación de acciones al administrador Biostar2

Nombre del Tratamiento	Fortalecimiento en la asignación de usuarios alternos sobre el sistema
Descripción del tratamiento	Asignación y nombramiento de usuarios que tengan los mismos privilegios que el administrador sobre el sistema.
Riesgo Asociado	R41
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A..18.1.3 Protección de los registros
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen la creación de usuarios alternos con el rol de administrador Biostar2.
2	Procedimiento de creación de usuarios alternos con el rol de administrador Biostar2 sobre el sistema.
3	Evidenciar los permisos asignados al usuario alterno con rol de administrador Biostar2.
4	Identificar el registro y cancelación del usuario administrador de Biostar2, limitando por tiempo las acciones sobre el sistema Biostar2.
5	Controlar a que datos puede tener acceso el administrador de Biostar2.
6	Crear una cláusula contractual que permita establecer las obligaciones del debido control del administrador del aplicativo Biostar2.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 37 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la suplantación de la identidad del administrador Biostar2 sobre la plataforma.

Cuadro 37. Pérdida de disponibilidad por suplantación al administrador Biostar2

Nombre del Tratamiento	Fortalecimiento de procedimientos de autenticación de usuario
Descripción del tratamiento	Actualización de los controles de autenticación de usuarios sobre los sistemas.
Riesgo Asociado	R42
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.18.1.4 Protección de los datos y privacidad de la información personal
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen varios mecanismos de autenticación al administrador de Biostar2 dentro del sistema.
2	Procedimiento de creación de usuario administrador Biostar2 con varios mecanismos de autenticación.
3	Evidenciar los permisos asignados al usuario administrador Biostar2.
4	Se debe determinar las reglas de control de acceso al Biostar2, así como los derechos y las restricciones de acuerdo con el rol administrador Biostar2.
5	Utilización de gestión de información de autenticación secreta del administrador Biostar2.
6	Para verificación de la identidad y autenticación fuerte del rol administrador Biostar2, debería usarse métodos de autenticación distintos a las contraseñas, como tarjetas inteligentes, tokens o medios biométricos
7	Establecer procedimientos de autentificación del administrador Biostar2 robustas, asegurando que quien intenta utilizar los recursos es quien debería ser.
8	En el aplicativo debe existir un enlace visible a la información del tratamiento de datos personales del administrador del aplicativo Biostar2.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 38 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia del administrador de la plataforma Arquero.

Cuadro 38. Pérdida de disponibilidad por ausencia del administrador Arquero

Nombre del Tratamiento	Fortalecimiento en la asignación de personal de respaldo
Descripción del tratamiento	Asignación y nombramiento de personal que asuma los roles clave que presenten ausencia
Riesgo Asociado	R43
Controles Asociados	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.1.2 Términos y condiciones del empleo A.12.1.1 Procedimientos documentados de operación
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas de respaldo del administrador de Arquero para la prestación del servicio TI “control de acceso.”
2	Crear mecanismos de obligatoriedad en la asistencia a las capacitaciones referentes a la seguridad de la información por parte del rol administrador de Arquero.
3	Crear mecanismos contractuales para el rol administrador Arquero para el cumplimiento de las funciones referentes a la seguridad.
4	Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían respaldar en caso de que el administrador de Arquero no pueda ejercer sus responsabilidades, afectando la continuidad del servicio TI.
5	Activar a aquellos colaboradores que sean respaldo del administrador de Arquero, en caso de que este no pueda ejercer sus responsabilidades.
6	Preparación de la ausencia prolongada del administrador de Arquero por enfermedad personal y/o familiar, por aplicación de medidas de protección como el aislamiento obligatorio o por la interrupción o disminución del transporte público.
7	Habilitar procedimientos que permitan que el administrador de Arquero pueda realizar sus actividades por medio del teletrabajo, con horario flexible o con alternancia.
8	Crear procedimiento documentado de las actividades realizadas por el administrador del sistema Arquero.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Contratos laborales
Fuente: Elaboración propia	

En el cuadro 39 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la negación sobre las acciones y funciones del administrador de la plataforma Arquero.

Cuadro 39. Pérdida de disponibilidad por negación de acciones al administrador Arquero

Nombre del Tratamiento	Fortalecimiento en la asignación de usuarios alternos sobre el sistema
Descripción del tratamiento	Asignación y nombramiento de usuarios que tengan los mismos privilegios que el administrador sobre el sistema.
Riesgo Asociado	R44
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.13.1.1 Controles de red

Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen la creación de usuarios alternos con el rol de administrador Arquero.
2	Procedimiento de creación de usuarios alternos con el rol de administrador Arquero sobre el sistema.
3	Evidenciar los permisos asignados al usuario alterno con rol de administrador Arquero.
4	Identificar el registro y cancelación del usuario administrador de Arquero, limitando por tiempo las acciones sobre el sistema Arquero.
5	Controlar a que datos puede tener acceso el administrador de Arquero.
6	Asegurar que la red posee un sistema de monitoreo y registro relacionados con el acceso del administrador del aplicativo Arquero.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad

Fuente: Elaboración propia

En el cuadro 40 que se muestra a continuación, se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la suplantación de la identidad del administrador BMS Arquero sobre la plataforma.

Cuadro 40. Pérdida de disponibilidad por suplantación al administrador BMS Arquero

Nombre del Tratamiento	Fortalecimiento de procedimientos de autenticación de usuario
Descripción del tratamiento	Actualización de los controles de autenticación de usuarios sobre los sistemas.
Riesgo Asociado	R45
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.13.1.2 Seguridad de los servicios de red
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen varios mecanismos de autenticación al administrador de BMS Arquero dentro del sistema.
2	Procedimiento de creación de usuario administrador Arquero con varios mecanismos de autenticación.
3	Evidenciar los permisos asignados al usuario administrador BMS Arquero.
4	Se debe determinar las reglas de control de acceso al BMS Arquero, así como los derechos y las restricciones de acuerdo con el rol administrador BMS Arquero.
5	Utilización de gestión de información de autenticación secreta del administrador BMS Arquero.
6	Para verificación de la identidad y autenticación fuerte del rol administrador BMS Arquero, debería usarse métodos de autenticación distintos a las contraseñas, como tarjetas inteligentes, tokens o medios biométricos
7	Establecer procedimientos de autentificación del administrador BMS Arquero robustas, asegurando que quien intenta utilizar los recursos es quien debería ser.
8	Asegurar con acuerdos de gestión la calidad de los servicios de red relacionados con el acceso al administrador del aplicativo Arquero.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 41 ilustrado a continuación, se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia del administrador de hardware.

Cuadro 41. Pérdida de disponibilidad por ausencia del administrador hardware

Nombre del Tratamiento	Fortalecimiento en la asignación de personal de respaldo
Descripción del tratamiento	Asignación y nombramiento de personal que asuma los roles clave que presenten ausencia
Riesgo Asociado	R46
Controles Asociados	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.1.2 Términos y condiciones del empleo A.8.1.4 Devolución de activos
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas de respaldo del administrador de hardware para la prestación del servicio TI “control de acceso.”
2	Crear mecanismos de obligatoriedad en la asistencia a las capacitaciones referentes a la seguridad de la información por parte del rol administrador de hardware.
3	Crear mecanismos contractuales para el rol administrador de hardware para el cumplimiento de las funciones referentes a la seguridad.
4	Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían respaldar en caso de que el administrador de hardware no pueda ejercer sus responsabilidades, afectando la continuidad del servicio TI.
5	Activar a aquellos colaboradores que sean respaldo del administrador de hardware, en caso de que este no pueda ejercer sus responsabilidades.
6	Preparación de la ausencia prolongada del administrador de hardware por enfermedad personal y/o familiar, por aplicación de medidas de protección como el aislamiento obligatorio o por la interrupción o disminución del transporte público.
7	Habilitar procedimientos que permitan que el administrador de hardware pueda realizar sus actividades por medio del teletrabajo, con horario flexible o con alternancia.
8	Formalizar proceso de finalización de contrato donde se devuelvan todos los activos de la organización.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Contratos laborales
Fuente: Elaboración propia	

En el cuadro 42 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la negación sobre las acciones y funciones del administrador de hardware.

Cuadro 42. Pérdida de disponibilidad por negación de acciones al administrador de hardware

Nombre del Tratamiento	Fortalecimiento en la asignación de usuarios alternos sobre el sistema
Descripción del tratamiento	Asignación y nombramiento de usuarios que tengan los mismos privilegios que el administrador sobre el sistema.
Riesgo Asociado	R47
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.10.1.2 Gestión de Claves
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen la creación de usuarios alternos con el rol de administrador de hardware.
2	Procedimiento de creación de usuarios alternos con el rol de administrador de hardware sobre el sistema.
3	Evidenciar los permisos asignados al usuario alterno con rol de administrador de hardware.
4	Identificar el registro y cancelación del usuario administrador de hardware, limitando por tiempo las acciones sobre los diferentes sistemas.
5	Controlar a que datos puede tener acceso el administrador de hardware.
6	Creación de política para la gestión de claves teniendo en cuenta todo el ciclo de vida de las claves.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 43 se documentan las siete estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la suplantación de la identidad del administrador de hardware.

Cuadro 43. Pérdida de disponibilidad por suplantación al administrador hardware

Nombre del Tratamiento	Fortalecimiento de procedimientos de autenticación de usuario
Descripción del tratamiento	Actualización de los controles de autenticación de usuarios sobre los sistemas.
Riesgo Asociado	R48
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.7.2.2 Concientización, educación, y formación en seguridad de la información
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen varios mecanismos de autenticación al administrador de hardware dentro del sistema.
2	Procedimiento de creación de usuario administrador de hardware con varios mecanismos de autenticación.
3	Evidenciar los permisos asignados al usuario administrador de hardware.
4	Utilización de gestión de información de autenticación secreta del administrador de hardware.
5	Para verificación de la identidad y autenticación fuerte del rol administrador de hardware, debería usarse métodos de autenticación distintos a las contraseñas, como tarjetas inteligentes, tokens o medios biométricos
6	Establecer procedimientos de autentificación del administrador de hardware robustas, asegurando que quien intenta utilizar los recursos es quien debería ser.
7	Realizar formación en temas relacionados con la seguridad de la información protección de claves y gestión de control de acceso.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 44 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia del administrador de la NAS.

Cuadro 44. Pérdida de disponibilidad por ausencia del administrador NAS

Nombre del Tratamiento	Fortalecimiento en la asignación de personal de respaldo
Descripción del tratamiento	Asignación y nombramiento de personal que asuma los roles clave que presenten ausencia
Riesgo Asociado	R49
Controles Asociados	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.1.2 Términos y condiciones del empleo A.6.1.2 Segregación de funciones
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas de respaldo del administrador NAS para la prestación del servicio TI “control de acceso.”
2	Crear mecanismos de obligatoriedad en la asistencia a las capacitaciones referentes a la seguridad de la información por parte del rol administrador NAS
3	Crear mecanismos contractuales para el rol administrador NAS para el cumplimiento de las funciones referentes a la seguridad.
4	Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían respaldar en caso de que el administrador de la NAS no pueda ejercer sus responsabilidades, afectando la continuidad del servicio TI.
5	Activar a aquellos colaboradores que sean respaldo del administrador NAS, en caso de que este no pueda ejercer sus responsabilidades.
6	Preparación de la ausencia prolongada del administrador NAS por enfermedad personal y/o familiar, por aplicación de medidas de protección como el aislamiento obligatorio o por la interrupción o disminución del transporte público.
7	Habilitar procedimientos que permitan que el administrador NAS pueda realizar sus actividades por medio del teletrabajo, con horario flexible o con alternancia.
8	Establecer controles de seguimiento y monitoreo en tiempo real para garantizar si está administrando la NAS por el usuario correcto.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Contratos laborales
Fuente: Elaboración propia	

En el cuadro 45 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la negación sobre las acciones y funciones del administrador de la NAS.

Cuadro 45. Pérdida de disponibilidad por negación de acciones al administrador NAS

Nombre del Tratamiento	Fortalecimiento en la asignación de usuarios alternos sobre el sistema
Descripción del tratamiento	Asignación y nombramiento de usuarios que tengan los mismos privilegios que el administrador sobre el sistema.
Riesgo Asociado	R50
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.13.2.4 Acuerdos de confidencialidad y de no divulgación
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen la creación de usuarios alternos con el rol de administrador NAS.
2	Procedimiento de creación de usuarios alternos con el rol de administrador NAS sobre el sistema.
3	Evidenciar los permisos asignados al usuario alterno con rol de administrador NAS
4	Identificar el registro y cancelación del usuario administrador NAS, limitando por tiempo las acciones sobre la NAS.
5	Controlar a que datos puede tener acceso el administrador de la NAS.
6	Crear acuerdo de confidencialidad para los terceros que gestionen la NAS cuando el administrador no tenga acceso a la misma.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 46 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la suplantación de la identidad del administrador de la NAS.

Cuadro 46. Pérdida de disponibilidad por suplantación al administrador NAS

Nombre del Tratamiento	Fortalecimiento de procedimientos de autenticación de usuario
Descripción del tratamiento	Actualización de los controles de autenticación de usuarios sobre los sistemas.
Riesgo Asociado	R51
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.18.1.4 Protección de los datos personales y privacidad de la información

Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen varios mecanismos de autenticación al administrador NAS dentro del sistema.
2	Procedimiento de creación de usuario administrador NAS con varios mecanismos de autenticación.
3	Evidenciar los permisos asignados al usuario administrador NAS.
4	Se debe determinar las reglas de control de acceso a la NAS, así como los derechos y las restricciones de acuerdo con el rol administrador de la NAS.
5	Utilización de gestión de información de autenticación secreta del administrador de la NAS.
6	Para verificación de la identidad y autenticación fuerte del rol administrador de la NAS, debería usarse métodos de autenticación distintos a las contraseñas, como tarjetas inteligentes, tokens o medios biométricos
7	Establecer procedimientos de autentificación del administrador de la NAS robustas, asegurando que quien intenta utilizar los recursos es quien debería ser.
8	Establecer controles para cumplir con legislación vigente en protección de datos personales almacenados en la NAS.

Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 47 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia del administrador del CCTV.

Cuadro 47. Pérdida de disponibilidad por ausencia del administrador CCTV

Nombre del Tratamiento	Fortalecimiento en la asignación de personal de respaldo
Descripción del tratamiento	Asignación y nombramiento de personal que asuma los roles clave que presenten ausencia
Riesgo Asociado	R52
Controles Asociados	A.7.2.1 Responsabilidades de la dirección A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.7.1.2 Términos y condiciones del empleo A.16.1.1 Responsabilidades y procedimientos
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas de respaldo del administrador CCTV para la prestación del servicio TI “control de acceso.”
2	Crear mecanismos de obligatoriedad en la asistencia a las capacitaciones referentes a la seguridad de la información por parte del rol administrador CCTV.
3	Crear mecanismos contractuales para el rol administrador CCTV para el cumplimiento de las funciones referentes a la seguridad.
4	Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían respaldar en caso de que resultado de que el administrador CCTV no pueda ejercer sus responsabilidades, afectando la continuidad del servicio TI.
5	Activar a aquellos colaboradores que sean respaldo del administrador CCTV, en caso de que este no pueda ejercer sus responsabilidades.
6	Preparación de la ausencia prolongada del administrador CCTV por enfermedad personal y/o familiar, por aplicación de medidas de protección como el aislamiento obligatorio o por la interrupción o disminución del transporte público.
7	Habilitar procedimientos que permitan que el administrador CCTV pueda realizar sus actividades por medio del teletrabajo, con horario flexible o con alternancia.
8	Establecer a la persona responsable de cubrir en caso de ausencia del administrador de CCTV.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Contratos laborales
Fuente: Elaboración propia	

En el cuadro 48 se documentan las seis estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la negación sobre las acciones y funciones del administrador del CCTV.

Cuadro 48. Pérdida de disponibilidad por negación de acciones al administrador CCTV

Nombre del Tratamiento	Fortalecimiento en la asignación de usuarios alternos sobre el sistema	
Descripción del tratamiento	Asignación y nombramiento de usuarios que tengan los mismos privilegios que el administrador sobre el sistema.	
Riesgo Asociado	R53	
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.13.1.3 Separación de redes	
Estrategias por Realizar		
Estrategia	Descripción	
1	Creación de políticas que enmarquen la creación de usuarios alternos con el rol de administrador CCTV.	
2	Procedimiento de creación de usuarios alternos con el rol de administrador CCTV sobre el sistema de CCTV	
3	Evidenciar los permisos asignados al usuario alterno con rol de administrador CCTV	
4	Identificar el registro y cancelación del usuario administrador CCTV, limitando por tiempo las acciones sobre el CCTV.	
5	Controlar a que datos puede tener acceso el administrador de CCTV.	
6	Segmentación de la red en donde se encuentre los equipos del CCTV.	
Duración estimada del tratamiento del riesgo	1 año	
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad	
Fuente: Elaboración propia		

En el cuadro 49 se documentan las ocho estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la suplantación de la identidad del administrador del CCTV.

Cuadro 49. Pérdida de disponibilidad por suplantación al administrador CCTV

Nombre del Tratamiento	Fortalecimiento de procedimientos de autenticación de usuario
Descripción del tratamiento	Actualización de los controles de autenticación de usuarios sobre los sistemas.
Riesgo Asociado	R54
Controles Asociados	A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.10.1.1 Política sobre el empleo de controles criptográficos
Estrategias por Realizar	
Estrategia	Descripción
1	Creación de políticas que enmarquen varios mecanismos de autenticación al administrador CCTV dentro del sistema.
2	Procedimiento de creación de usuario administrador CCTV con varios mecanismos de autenticación.
3	Evidenciar los permisos asignados al usuario administrador CCTV.
4	Se debe determinar las reglas de control de acceso al CCTV, así como los derechos y las restricciones de acuerdo con el rol administrador del CCTV.
5	Utilización de gestión de información de autenticación secreta del administrador del CCTV.
6	Para verificación de la identidad y autenticación fuerte del rol administrador del CCTV, debería usarse métodos de autenticación distintos a las contraseñas, como tarjetas inteligentes, tokens o medios biométricos.
7	Establecer procedimientos de autentificación del administrador del CCTV robustas asegurando que quien intenta utilizar los recursos es quien debería ser.
8	Establecer una política de almacenamiento de contraseñas donde se tenga un algoritmo de encriptación fuerte.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Políticas de seguridad
Fuente: Elaboración propia	

En el cuadro 50 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo router.

Cuadro 50. Pérdida de disponibilidad del router por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R57
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.15.1.3 Cadena de suministro de tecnologías de la información y las comunicaciones
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico del router en caso de ser requerido.
2	Instalación de las UPS al servicio del router previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan el router realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Establecer en la cadena de suministro con proveedores los tiempos máximos de entrega del servicio de energía eléctrica.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS
Fuente: Elaboración propia	

En el cuadro 51 se documentan las cuatro estrategias y los cuatro controles establecidos que buscan mitigar y tratar el riesgo asociado a la pérdida de disponibilidad causada por la ausencia de energía eléctrica sobre el activo de información tipo switch.

Cuadro 51. Pérdida de disponibilidad del switch por ausencia de fluido eléctrico

Nombre del Tratamiento	Fortalecimiento de infraestructura de respaldo eléctrico
Descripción del tratamiento	Asignación de ups que permita la continuidad del fluido eléctrico para los activos de información del servicio TI "control de acceso"
Riesgo Asociado	R60
Controles Asociados	A.11.2.2 Servicios de suministro A.12.1.3 Gestión de capacidad A.11.2.4 Mantenimiento de equipos A.18.2.3 Revisión del cumplimiento técnico
Estrategias por Realizar	
Estrategia	Descripción
1	Adquisición de UPS que cumplan con las especificaciones mínimas requeridas para soportar el fluido eléctrico del switch en caso de ser requerido.
2	Instalación de las UPS al servicio del switch previamente adquiridas.
3	Fortalecer los planes de mantenimiento preventivos y correctivos sobre las UPS que soportan el switch realizándolos en un periodo de tiempo más corto con respecto a los tiempos actuales.
4	Establecer medidas correctivas a los fallos presentados en lo relacionado con el fluido eléctrico para el switch.
Duración estimada del tratamiento del riesgo	1 año
Recursos necesarios para el tratamiento del riesgo	Personas: funcionarios Grow Data Documentación: Manuales de instalación Equipos: UPS
Fuente: Elaboración propia	

5.7 ANÁLISIS DE IMPACTO AL NEGOCIO

Esta sección presenta los datos del Análisis de Impacto al Negocio – BIA (Business Impact Analysis) realizado en Grow Data, donde se describe la información identificada en la fase del levantamiento de la información aplicada en conjunto con el personal clave de Grow Data.

Igualmente se evidencian los impactos en caso de que se interrumpan las actividades a causa de un evento o catástrofe natural, los cuales son: reputación y financiera para la Entidad, esta última teniendo en cuenta el presupuesto que la prestación del servicio TI representa para Grow Data, el cual establece un ingreso de $30.000.000 mensuales. Esto se lleva a cabo a través de la aplicación de fórmulas para definir índices de prioridad en el Análisis de Impacto al Negocio – BIA, y así llevar a la creación del plan de contingencia del servicio TI.

Para brindar un mejor entendimiento del Análisis de Impacto al Negocio realizado en Grow Data, se describen cada uno de los puntos que fueron valorados:

5.8 DATOS DEL SERVICIO TI “CONTROL DE ACCESO”

En este punto se realiza la identificación del personal clave para la prestación del servicio TI “control de acceso”, en el cuadro 52 se presenta la información identificada del personal clave (nombre, cargo y e-mail) de Grow Data para el servicio TI “control de acceso”.

Cuadro 52. Personal clave identificado en el BIA

Nombre	Cargo	E-mail
José Rodríguez Toro	Líder del Servicio	jose.rodriguez@growdata.com.co
	Administrador Biostar2	
	Administrador BMS ARQUERO	
	Administrador de Redes	
	Administrador NAS	
	Administrador CCTV	
Kenny Quintero	Administrador de Hardware	kenny.quintero@growdata.com.co
Fuente: Elaboración propia		

5.9 ENTRADAS, SALIDAS E IMPACTOS

En este punto se realiza la identificación de aquellas entradas necesarias para que el servicio TI “control de acceso” pueda cumplir con los objetivos dentro de la operación, así como también las salidas resultantes de la operación del servicio TI. Adicionalmente se establecen los impactos a nivel de reputación y financieros a los cuales Grow Data se podría ver expuesto en caso de que no se pueda ofrecer el servicio TI. A continuación, se detallan cada uno de estos puntos:

5.9.1 Entradas. Identificación de las entradas de las actividades críticas establecidas con sus parámetros necesarios como son (Actividad – Activo de información – Descripción – Medio de Recepción), en el cuadro 53 se documenta la información de las entradas de estas actividades críticas.

Cuadro 53. Identificación de las entradas de las actividades criticas

Actividad	Activo de información	Descripción	Medio recepción
Captura de datos biométricos de las personas que desean ingresar a las instalaciones	BMS Arquero	Datos dactilares	Archivos digitales
Mantenimientos Preventivos al Hardware	Activos de Información tipo hardware	Datos de la ubicación de los equipos / Persona de contacto / Autorización de ingreso de personal	Medio de Comunicación Oficial
Mantenimientos correctivos al Hardware	Activos de Información tipo hardware	Personal capacitado para realizar el tipo de correcciones necesarias / autorización de ingreso del personal	Medio de Comunicación Oficial
Backup aplicaciones	Bases de datos	conocimiento en bases de datos y aplicaciones de control de acceso	Bases de Datos
Monitoreo de los servicios	Software del fabricante (HIKVISION, BIOSTAR 2, ARQUERO, SPOT,24 SATELITAL)	check de servicios	Físico Directo

Cuadro 53. (Continuación)

Actividad	Activo de información	Descripción	Medio recepción
Actualización de aplicaciones	Software del fabricante (HIKVISION, BIOSTAR 2, ARQUERO, SPOT,24 SATELITAL)	upgrade de las nuevas versiones disponibles	Medio de Comunicación Oficial
Simulacros de alarmas	Hardware de las sedes principales	funcionamiento del servicio	Físico Directo
Servicios de GPS y Satelital (SPOT)	Software y servicios de monitoreo	rastreo GPS	Físico Directo
Fuente: Elaboración propia			

5.9.2 Salidas. Identificación de las salidas de las actividades críticas establecidas con sus parámetros necesarios como son (Actividad – Activo de información – Descripción – Medio de Salida), en el cuadro 54 se documenta la información de las salidas de estas actividades críticas.

Cuadro 54. Identificación de las salidas de las actividades críticas

Actividad	Activo de información	Descripción	Medio salida
Captura de datos biométricos de las personas que desean ingresar a las instalaciones	BMS Arquero	Perfil de acceso	Archivos digitales
Mantenimientos Preventivos al Hardware	Activos de Información tipo hardware	Check List de estado de equipos	Archivos digitales
Mantenimientos correctivos al Hardware	Activos de Información tipo hardware	Reparación equipos de seguridad electrónica	Archivo físico
Backup aplicaciones	Bases de datos	base de datos	Archivos digitales
Monitoreo de los servicios	Software del fabricante (HIKVISION, BIOSTAR 2, ARQUERO, SPOT,24 SATELITAL)	Check List de estado de equipos	Archivo físico

Cuadro 54. (Continuación)

Actividad	Activo de información	Descripción	Medio salida
simulacros de alarmas	Hardware de las sedes principales	pruebas de funcionamiento	Archivo físico
actualización de aplicaciones	Software del fabricante (HIKVISION, BIOSTAR 2, ARQUERO, SPOT,24 SATELITAL)	nuevas versiones	Archivo físico
Servicios de GPS y Satelital (SPOT)	Software y servicios de monitoreo	plataforma de administración	Archivos digitales
Fuente: Elaboración propia			

5.9.3 Impactos. Identificación de los impactos reputacionales y financieros de cada una de las actividades críticas enfocadas en la entrega del servicio TI “Control de acceso” por parte de Grow Data a su cliente. Para un mejor entendimiento de los impactos analizados, en el cuadro 55 se establecen los valores y su descripción establecidos para el presente BIA.

Cuadro 55. Identificación de los impactos reputacionales y financieros

Impacto reputacional	Descripción	Valoración	Impacto financiero	Descripción	Valoración
Catastrófico	Se impacta la reputación de la entidad afectando la imagen a nivel Nacional o Global	5	Catastrófico	Impacto que afecte la ejecución presupuestal en la prestación del servicio TI “Control de acceso” en un valor mayor o igual al 50%	5
Mayor	Se impacta la reputación de la entidad afectando la imagen ante los organismos del estado	4	Mayor	Impacto que afecte la ejecución presupuestal en la prestación del servicio TI “Control de acceso” en un valor mayor o igual al 20%	4

Cuadro 55. (Continuación)

Impacto reputacional	Descripción	Valoración	Impacto financiero	Descripción	Valoración
Moderado	Se impacta la reputación de la entidad afectando la imagen ante entes reguladores	3	Moderado	Impacto que afecte la ejecución presupuestal en la prestación del servicio TI "Control de acceso" en un valor mayor o igual al 5%	3
Menor	Se impacta la reputación de la entidad afectando la imagen a nivel contractual (GrowData - Entidad)	2	Menor	Impacto que afecte la ejecución presupuestal en la prestación del servicio TI "Control de acceso" en un valor mayor o igual al 1%	2
Insignificante	Se impacta la reputación al interior de la Entidad	1	Insignificante	Impacto que afecte la ejecución presupuestal en la prestación del servicio TI "Control de acceso" un valor mayor o igual al 0.5%	1
Fuente: Elaboración propia					

De los impactos identificados en el BIA, se desglosan por cada actividad crítica identificada la valoración de aquellos impactos a nivel reputacional y financiero a los que Grow Data puede verse afectado si estas actividades críticas no se llegaran a realizar, la valoración total de impacto se calcula a través de un promedio, acercando el resultado a la calificación más alta de la valoración, en el cuadro 56 se muestra la valoración de estos impactos.

Cuadro 56. Valoración total impactos

Actividad crítica	Impacto reputacional	Impacto financiero	Valoración total impactos
Captura de datos biométricos de las personas que desean ingresar a las instalaciones	5	4	5

Cuadro 56. (Continuación)

Actividad crítica	Impacto reputacional	Impacto financiero	Valoración total impactos
Mantenimientos Preventivos al Hardware	2	3	3
Mantenimientos correctivos al Hardware	5	3	4
Backup aplicaciones	1	3	2
Monitoreo de los servicios	4	3	4
actualización de aplicaciones	1	2	2
simulacros de alarmas	3	2	3
Servicios de GPS y Satelital (SPOT)	3	2	3
Fuente: Elaboración propia			

5.10 ROLES Y RESPONSABILIDADES

Una vez se tiene las estrategias definidas en el tratamiento de riesgos que buscan brindar la continuidad de acuerdo con los diferentes riesgos identificados, se establecen aquellos responsables que aseguren la efectividad de estas estrategias, en el cuadro 57, se detallan los roles y responsabilidades necesarios para ejecutar el presente plan de contingencia.

Cuadro 57. Roles equipo de recuperación

Equipo de Recuperación	Líder del Equipo	Líder de servicio TI
	Recuperador de Hardware	Administrador de Hardware
		Administrador de Redes
		Administrador NAS
		Administrador CCTV
		Administrador de intrusión y detección de incendios
	Recuperador de Software	Administrador Biostar2
		Administrador BMS Arquero
	Equipo de Comunicación	Administrador de Redes
Fuente: Elaboración propia		

5.10.1 Equipo de recuperación. La conformación de este equipo está encaminado a determinar las responsabilidades necesarias para recuperar el servicio TI ante la materialización de un evento o catástrofe que pueda afectar su operación normal. Este equipo de recuperación tiene las siguientes responsabilidades:

- Definir controles que puedan prevenir y/o disminuir la probabilidad de ocurrencia.

- Establecer, probar, y actualizar el Plan de Contingencia del servicio TI “Control de acceso”.
- Recuperar el servicio TI en el menor tiempo posible y teniendo en cuenta los tiempos de recuperación identificados.
- Generar los informes respectivos cuando se materialice un evento que afecte la operación normal del servicio TI

Teniendo en cuenta lo anterior, se establecen las funciones de los diferentes integrantes del equipo de recuperación:

5.10.2 Equipo Líder (LE). A continuación, se establecen las responsabilidades de este rol.

- Tomar la decisión de activar el plan de contingencia teniendo en cuenta el diagnóstico realizado a la incidencia y a los criterios de activación.
- Liderar las actividades de los demás integrantes que conforman el equipo de recuperación validando que el personal se encuentra disponible y activo para ejecutar las actividades propias requeridas para la recuperación del servicio TI.
- Determinar el nivel de desastre cuando se materializa el evento o catástrofe realizando una revisión de los activos de TI afectados por el evento mediante un check list de validación.
- Tomar la decisión de salir de contingencia y volver a la normalidad teniendo en cuenta los criterios de vuelta a la normalidad.

5.10.3 Recuperador de hardware (RH). Las responsabilidades de este rol se describen a continuación:

- Identificar el Hardware que resultó afectado por la materialización del evento o catástrofe mediante la validación y revisión física y funcional de cada uno de los componentes de hardware, apoyándose en el formato Matriz_Revisión_Física_Tecnica_hardware.xlsx, así:

  - Tipo de componente de hardware
  - Estado físico componente de hardware
  - Estado Disco Duro componente de hardware
  - Estado tarjeta de memoria RAM componente de hardware
  - Estado componentes eléctricos
  - Estado lector de huellas
  - Estado cableado de red
  - Estado cableado eléctrico
  - Estado lente de cámara
  - Estado sensores

- Estado pantalla
- Estado sistema resortado

- Coordinar con los diferentes proveedores del hardware que se dé cumplimiento a los contratos de mantenimiento, contactando vía correo y telefónicamente a los representantes de estos proveedores para solicitar dichos mantenimientos correctivos del hardware validado en el punto anterior.
- Comprobar el correcto funcionamiento del hardware que fue remplazado y/o arreglado por los proveedores, validando su estado físico y funcional, de acuerdo con el formato Matriz_Revisión_Física_Tecnica_hardware.xlsx.
- Suministrar el Backup requerido para operar el servicio TI “Control de acceso” bajo contingencia, brindando acceso a la información almacenada en la NAS del servicio TI.

5.10.4 Recuperador de software (RS). Para este rol, se establecen las siguientes responsabilidades:

- Identificar bases de datos y aplicaciones que han sido afectados en la materialización del evento o catástrofe, de acuerdo con el inventario de las bases de datos y aplicaciones documentados en el archivo Inventario_aplicaciones _bases_de_datos_control_acceso.xlsx
- Suministrar el software necesario para la restauración del servicio TI “Control de acceso”, brindando los ejecutables actualizados de las aplicaciones y/o bases de datos.
- Instalar y configurar el software que fue afectado por la materialización del evento o catástrofe, apoyándose en los manuales de instalación actualizados del software requerido a instalar.

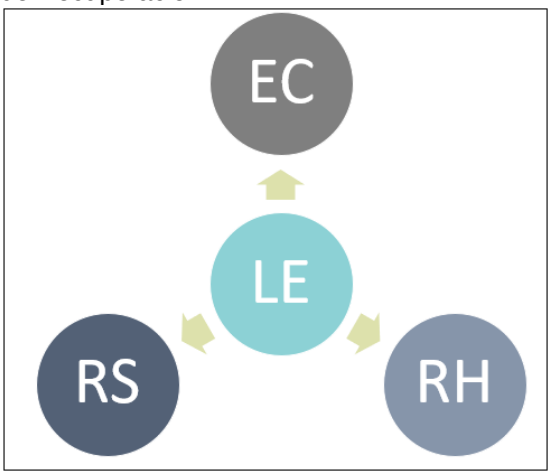
5.10.5 Equipo de comunicación (EC). Las actividades y responsabilidades para este rol se enlistan de la siguiente manera:

- Comunicar oficialmente a las partes interesadas la ejecución del plan de contingencia del servicio TI “Control de acceso” teniendo en cuenta el árbol de llamadas y los diferentes medios de comunicación (redes sociales, llamadas telefónicas, correo electrónico, etc.) disponibles.
- Comunicar oficialmente a las partes interesadas la vuelta de la operación a la normalidad teniendo en cuenta los diferentes medios de comunicación (redes sociales, llamadas telefónicas, correo electrónico, etc.) disponibles.

En la figura 3 se ilustra la relación entre los distintos roles que se han establecido durante la contingencia. Se puede observar que el rol principal dentro del equipo de recuperación es el líder del equipo, quien tiene la responsabilidad de coordinar, proporcionar directrices y supervisar la ejecución de las actividades de los demás

roles, tales como el equipo de recuperación de software, el equipo de recuperación de hardware y el equipo de comunicación:

Figura 3. Relación Equipo de Recuperación



Fuente: Elaboración propia

5.11 RECURSOS DE RECUPERACIÓN

Se identifican aquellos recursos necesarios (personas, hardware, software, documentos, etc.) para que el servicio pueda ser recuperado en el menor tiempo posible y cumpliendo con los tiempos de recuperación establecidos en el Análisis de Impacto al Negocio, en el cuadro 58 se documentan los recursos de recuperación para el servicio TI “control de acceso”.

Cuadro 58. Recursos de recuperación

Cargo / Rol	Software	Documentación
Administrador Biostar2	MySQL	Manual Base de datos Manual Aplicación
Administrador BMS Arquero	ORACLE, MARIA DB, MYSQL	Manual Base de datos Manual Aplicación
Administrador de Redes	-	Manual Subnetting
Administrador de Hardware	Sistema Operativo (S.O)	Manual de instalación y configuración S.O
Administrador NAS	HIKCENTRAL	Manual de instalación y configuración NAS
Administrador CCTV	IVMS 4200	Manual de instalación y configuración CCTV
Fuente: Elaboración propia		

5.12 ASIGNACIÓN DE ROLES

Teniendo en cuenta los recursos de recuperación (personas) identificados en el Análisis de Impacto al Negocio, se establece en el cuadro 59 la asignación de los roles dentro del equipo de recuperación propuesto alineado con los roles existentes dentro de Grow Data.

Cuadro 59. Identificación de roles

Rol equipo de recuperación	Rol Grow Data
Líder del Equipo (LE)	Líder del Servicio TI
Recuperación de Hardware (RH)	Administrador de Hardware
Recuperación de Software (RS)	Administrador Biostar2
Equipo de Comunicación (EC)	Administrador de Redes
Fuente: Elaboración propia	

5.12.1 Árbol de llamadas. Teniendo ya identificados los roles que serán los responsables de gestionar la operación en contingencia y la recuperación de los distintos servicios tecnológicos que apalancan la entrega del servicio TI “Control de acceso”, se establece la secuencia de comunicación que se activa de acuerdo con el activo que presente indisponibilidad, la cual permite tener una visión clara y detallada al momento de establecer una correcta y eficiente comunicación, optimizando el tiempo de recuperación. En el cuadro 60, se establece el árbol de llamadas.

Cuadro 60. Árbol de llamadas

Activo no Disponible	Responsable	Celular	Correo Electrónico
Biostar2	José Rodríguez	3217460932	jose.rodriguez@growdata.com.co
BMS Arquero			
Redes			
NAS			
CCTV			
Hardware	Kenny Quintero	3127746654	kenny.quintero@growdata.com.co
Fuente: Elaboración propia			

5.13 ACTIVIDADES ALTERNAS

En el cuadro 61 se identifican aquellas actividades que se encuentran establecidas cuando las actividades críticas no puedan ser ejecutadas de manera normal.

Cuadro 61. Actividades alternas

Tipo de actividad alterna	Justificación Tipo	Descripción de la actividad alterna
Semiautomático	Si no funcionan los lectores biométricos, se captura información en archivo Microsoft office	Se capturan los datos de los visitantes y funcionarios en un archivo de Excel.
	Pérdida de grabaciones en sedes territoriales	Se hace un llamado directo de las cámaras para obtener las grabaciones mediante la NAS (Network Attached Storage)
Totalmente manual	Si un control de acceso no funciona se debe hacer apertura de manera manual	En caso de emergencia o que algún usuario se quede encerrado se debe abrir de manera manual la puerta o molinetes
Fuente: Elaboración propia		

5.14 TIEMPOS DE RECUPERACIÓN

Para un mejor entendimiento de los tiempos de recuperación, en los siguientes subcapítulos se establecen los valores y su descripción establecidos para el BIA aplicados al servicio TI “Control de acceso” por Grow Data.

5.14.1 Identificación del RPO. El cual corresponde al tiempo que el servicio TI está dispuesto a perder de información o datos según el último punto de restauración o copia de seguridad que tengan de respaldo de los datos de información, en el cuadro 62 se muestra la respectiva valoración para medir el punto objetivo de recuperación del servicio TI.

Cuadro 62. Valoración RPO del servicio

Valoración RPO del servicio	Indicador	Descripción según la valoración del RPO
5	<=5 minutos	Para Grow Data, la tolerancia de perdida de información en los procedimientos o actividades no es permitida debido a la alta criticidad de los datos ingresados en el momento exacto del punto de interrupción.

Cuadro 62. (Continuación)

Valoración RPO del servicio	Indicador	Descripción según la valoración del RPO
4	<=1 hora	Para Grow Data, la tolerancia de perdida de información en los procedimientos o actividades es menor o igual a 1 hora de la generación de los datos ingresados y sus respectivos respaldos.
3	<=4 horas	Para Grow Data, la tolerancia de perdida de información en los procedimientos o actividades es de 4 horas de la generación de los datos ingresados, teniendo en cuenta la consolidación de los datos por día hábil y sus respectivos respaldos.
2	<=6 horas	Para Grow Data, la tolerancia de perdida de información en los procedimientos o actividades es de 6 horas de la generación de los datos ingresados, teniendo en cuenta la consolidación de los datos por semana en horarios hábiles y sus respectivos respaldos.
1	>8 horas	Para Grow Data, la tolerancia de perdida de información en los procedimientos o actividades es mayor de 8 horas de la generación de los datos ingresados, teniendo en cuenta las consolidaciones realizadas de forma diaria, mensual, bimestral, trimestral, semestral, anual de los datos y sus respectivos respaldos.
Fuente: Elaboración propia		

5.14.2 Identificación del RTO. El cual corresponde al tiempo que puede tolerar el servicio TI hasta reanudar nuevamente la operación después de una interrupción en sus actividades por causa de un evento o catástrofe natural, en el cuadro 63 se muestra la respectiva valoración para medir el tiempo objetivo de recuperación del servicio TI.

Cuadro 63. Valoración RTO del servicio

Valoración RTO del servicio	Indicador	Descripción según la valoración del RTO
5	<=5 minutos	La recuperación o restablecimiento de los procedimientos o actividades para Grow Data por una interrupción, deben ser inmediatos debido a la alta criticidad de la información.
4	<=1 hora	La recuperación o restablecimiento de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo menor a 1 hora debido a la criticidad de la información.
3	<=4 horas	La recuperación o restablecimiento de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo de 4 horas a 6 horas debido a la criticidad de la información.
2	<=6 horas	La recuperación o restablecimiento de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo de 6 horas a 8 horas debido a la criticidad de la información.
1	>8 horas	La recuperación o restablecimiento de los procedimientos o actividades por una interrupción pueden considerarse mayor a 8 horas debido que la información no es crítica para Grow Data.
Fuente: Elaboración propia		

5.14.3 Identificación del MAO. El cual corresponde al tiempo límite máximo que puede estar suspendida la entrega del servicio TI "control de acceso", en el cuadro 64 se muestra la respectiva valoración para medir la interrupción máxima aceptable del servicio TI.

Cuadro 64. Valoración MAO

Valoración MAO del servicio	Indicador	Descripción según la valoración del MAO
5	<=1 hora	Para Grow Data, la tolerancia de no entrega del servicio TI "Control de Acceso" en los procedimientos o actividades no es permitida debido a la alta criticidad de los datos ingresados en el momento exacto del punto de interrupción.
4	<=4 horas	Para Grow Data, la tolerancia de no entrega del servicio TI "Control de Acceso" en los procedimientos o actividades es menor o igual a 4 horas antes de producirse un deterioro inadmisible.
3	<=6 horas	Para Grow Data, la tolerancia de no entrega del servicio TI "Control de Acceso" en los procedimientos o actividades pueden considerarse dentro de un tiempo de 4 horas a 6 horas antes de producirse un deterioro inadmisible.

Cuadro 64. (Continuación)

Valoración MAO del servicio	Indicador	Descripción según la valoración del MAO
2	<=8 horas	Para Grow Data, la tolerancia de no entrega del servicio TI “Control de Acceso” en los procedimientos o actividades pueden considerarse dentro de un tiempo de 6 horas a 8 horas antes de producirse un deterioro inadmisible.
1	>8 horas	Para Grow Data, la tolerancia de no entrega del servicio TI “Control de Acceso” en los procedimientos o actividades puede considerarse mayor a 8 horas antes de producirse un deterioro inadmisible
Fuente: Elaboración propia		

5.14.4 Identificación del MTD. El cual corresponde al tiempo de inactividad máximo tolerable del servicio TI antes de causar a Grow Data consecuencias inaceptables, en el cuadro 65 se muestra la respectiva valoración para medir el tiempo de inactividad máximo tolerable del servicio TI.

Cuadro 65. Valoración MTD

Valoración MTD del servicio	Indicador	Descripción según la valoración del MTD
5	<=5 minutos	El tiempo máximo tolerable de los procedimientos o actividades para Grow Data por una interrupción, deben ser inmediatos antes de considerarse como inaceptable debido a la alta criticidad de entrega del servicio TI “Control de acceso”.
4	<=4 horas	El tiempo máximo tolerable de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo máximo de 4 horas antes de considerarse como inaceptable debido a la criticidad de la entrega del servicio TI “Control de acceso”.
3	<=8 horas	El tiempo máximo tolerable de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo de máximo 8 horas antes de considerarse como inaceptable debido a la criticidad de la entrega del servicio TI “Control de acceso”.
2	<=40 horas	El tiempo máximo tolerable de los procedimientos o actividades para Grow Data por una interrupción, pueden considerarse dentro de un tiempo máximo de 40 horas antes de considerarse como inaceptable debido a la criticidad de la entrega del servicio TI “Control de acceso”.
1	>40 horas	El tiempo máximo tolerable de los procedimientos o actividades por una interrupción, pueden considerarse mayor a 40 horas antes de considerarse como inaceptable debido que la criticidad de la entrega del servicio TI “Control de acceso”.
Fuente: Elaboración propia		

De acuerdo con el levantamiento del BIA y con la valoración de los tiempos de recuperación, en las siguientes tablas se presentan estos tiempos de recuperación identificados por Grow Data en la herramienta del BIA de acuerdo con la entrega del servicio TI “Control de acceso”.

5.14.5 Resultados tiempos de recuperación. El RPO está asociado a los procedimientos de respaldo de información definidos por Grow Data sobre el activo de información NAS, el RTO, el MAO y el MTD están asociados a la actividad critica de la captura de datos biométricos, la cual de acuerdo con Grow Data, esta actividad es la que presenta una gran importancia en la generación de valor del servicio TI ante sus clientes, en el cuadro 66 se presenta la evaluación de cada uno de estos tiempos de recuperación.

Cuadro 66. Resultados tiempos de recuperación

No. Actividad Crítica	Descripción	RPO	RTO	MAO	MTD
1	Activar los respaldos de información generadas de los aplicativos Biostar2, arquero y sus respectivas bases de datos.	**2**	**-**	**-**	**-**
2	Captura de datos biométricos de las personas que desean ingresar a las instalaciones.	**-**	**4**	**-**	**-**
	Captura de datos biométricos de las personas que desean ingresar a las instalaciones.	**-**	**-**	**3**	**-**
	Captura de datos biométricos de las personas que desean ingresar a las instalaciones.	**-**	**-**	**-**	**3**
Fuente: Elaboración propia					

Para la actividad crítica no. 1, la valoración del RPO se establece en 2, lo cual define que el tiempo máximo de información que Grow Data estaría dispuesto a perder durante una interrupción del servicio TI “control de acceso” es de seis (6) horas, teniendo en cuenta los procedimientos de respaldo de información que se deben realizar a los aplicativos Biostar2 y Arquero y a las bases de datos periódicamente; lo anterior obliga a que el administrador de la NAS gestione de manera correcta el desarrollo y la ejecución de los respaldos de información generada de la operación del servicio TI, asegurando que al momento de una interrupción al servicio TI, la información respaldada se encuentre lo más actualizada posible.

Para la actividad crítica no. 2, la valoración del RTO se establece en 4, lo cual define que el tiempo en que Grow Data debe volver a brindar la captura de los datos biométricos en un ambiente normal es de máximo seis (6) horas, tiempo en el cual se puede llegar a tolerar la indisponibilidad de esta captura de datos, sin llegar a afectar la continuidad y la oferta del servicio a sus clientes. Por lo anterior, Grow Data debe establecer este tiempo de nivel de servicio dentro de los contratos de la

prestación del servicio TI “Control de acceso” que suscrite con las diferentes entidades.

Para la actividad crítica no. 3, la valoración del MAO se establece en 3, lo cual define que el tiempo tolerable para la no lectura de los datos biométricos está establecida entre cuatro (4) a seis (6) horas, lo cual genera que Grow Data cuente con políticas y procedimientos que busquen no superar este umbral de tiempo cuando se presente indisponibilidad en los mecanismos de recopilación de datos biométricos.
Para la actividad critica no. 4, la valoración del MTD se establece en 3, lo cual define que la interrupción de la disponibilidad de la captura de datos biométricos no puede superar el umbral de ocho (8) horas, tiempo en el cual se impactaría de manera negativa la relación comercial que Grow Data tiene con las entidades a las cuales se les presta el servicio TI, provocando incumplimiento en las obligaciones contractuales y generando posibles sanciones económicas.

5.15 FASES ACTIVACIÓN PLAN DE CONTINGENCIA

Para poder ejecutar el plan de contingencia, se deben establecer las diferentes fases que guíen a Grow Data a tener un orden especifico en la ejecución de este, buscando cumplir con el manejo efectivo que se debe dar en la respuesta del evento que afecte la continuidad del servicio TI, en la siguiente figura 4 se establecen estas fases:

Figura 4. Fases plan de contingencia

Fuente: Elaboración propia

- **Detectar**: Fase que identifica un incidente, evento o catástrofe que puede causar indisponibilidad en el servicio TI “Control de acceso”, desarrollando los primeros pasos para el manejo del incidente, identificando los activos afectados, las actividades criticas afectadas, clasificación del incidente, etc., de acuerdo con el procedimiento de gestión de incidentes que Grow Data tiene documentado.
- **Diagnosticar**: Fase que identifica la naturaleza del incidente, evento o catástrofe, determinando la viabilidad de activar el plan de contingencia del servicio TI “Control de acceso” o, por lo contrario, gestionar la falla como un

incidente operativo “normal”, de acuerdo con el procedimiento de gestión de incidentes que Grow Data tiene documentado.

- **Activar**: Fase que desarrolla los pasos para activar el plan de contingencia de los servicios TI. Igualmente, para determinar si es necesaria la evacuación del personal de Grow Data, dependiendo si las instalaciones físicas donde se brinde el servicio TI “Control de acceso” no brinden las garantías de seguridad para el personal.
- **Operación en contingencia**: Fase que desarrolla los pasos cuando Grow Data se encuentre operando bajo contingencia.
- **Vuelta a la normalidad**: Fase que analiza las condiciones tecnológicas y físicas para decidir cuándo Grow Data volverá a operar bajo normalidad y recupera el servicio en el ambiente primario de operación.
- **Lecciones aprendidas**: Fase que Grow Data aprovecha el conocimiento obtenido durante el manejo del incidente, evento o catástrofe presentado, documentando que se hizo bien, que se hizo mal, puntos a mejorar, etc.

5.15.1 Criterios activación de contingencia. El equipo de recuperación debe tener en cuenta los siguientes componentes los cuales contienen los criterios mínimos, para cumplir y tomar la decisión correcta que determine la situación y entrar en contingencia:

- Componente Estratégico
  - La indisponibilidad del servicio TI “Control de Acceso” afecta de manera negativa el logro de los objetivos misionales de la prestación del servicio hacia las entidades.
  - El evento catastrófico afecta de manera parcial o total; generando indisponibilidad del servicio TI “Control de Acceso”.
  - El evento catastrófico puede llevar a Grow Data en incumplimientos contractuales que impacten de manera económica y reputacional.
- Componente Operativo
  - La integridad física del personal de Grow Data se encuentra en riesgo a causa del evento catastrófico.
  - La solución de la indisponibilidad del servicio TI puede superar los tiempos de recuperación definidos.
- Componente Tecnológico
  - El evento catastrófico puede llevar a presentar pérdida de información generada de la operación del servicio TI.
  - El evento catastrófico puede llegar a presentar indisponibilidad de los servidores que albergan los aplicativos y/o bases de datos que apalancan el servicio TI.
  - El evento catastrófico puede llegar a presentar indisponibilidad de las cámaras de vigilancia que detectan el personal que desea ingresar a las instalaciones donde se ofrece el servicio TI.

- El evento catastrófico puede llegar a presentar indisponibilidad de los lectores biométricos que recopilan las huellas de las personas que desean ingresar a las instalaciones donde se ofrece el servicio TI.

5.15.2 Criterios de vuelta a la normalidad. El líder del equipo de recuperación avala el retorno a "modo normalidad de operación" una vez se informa que están dadas las condiciones según lo establecido en los criterios de aceptación (Protocolos, Listas de chequeo, eliminación de alarmas). Igualmente debe de asegurar la vuelta a la normalidad teniendo en cuenta los siguientes componentes con sus respectivos criterios:

- Componente Estratégico
  - La falla generada por el evento catastrófico ya se encuentra solucionada.
  - La información procesada durante la operación bajo contingencia se encuentra identificada y consolidada.
- Componente Operativo
  - El personal de Grow Data cuenta con seguridad física para volver a operar en normalidad.
  - La hora es adecuada para realizar las actividades de operación necesarias y volver a retornar a la operación normal.
- Componente Tecnológico
  - Las bases de datos que apalancan el servicio TI se encuentran operativas.
  - La información alojada en las bases de datos se encuentra disponible.
  - La infraestructura tecnológica que soporta el servicio TI y de comunicación se encuentran operativos.
  - Los elementos básicos de seguridad informática están operativos y configurados.

5.15.3 Desarrollo del plan de contingencia. En el cuadro 67, se describen las actividades o procedimientos que se deben realizar en cada una de las fases del Plan de Contingencia del servicio TI "Control de acceso", donde se identifican los siguientes puntos:

- Fase: Identificar la fase en la cual corresponde la actividad (Detectar - Diagnosticar – Activar - Operación en contingencia - Vuelta a la normalidad - Lecciones aprendidas).
- Actividad: Define el flujo del procedimiento para ejecutar las actividades.
- Descripción de la Actividad: Acciones establecidas para gestionar el incidente o evento catastrófico.
- Responsable de la Actividad: Persona o grupo que tiene la responsabilidad de ejecutar las actividades relacionadas con la gestión del incidente.

- Entrada: Insumo necesarios que determinan las acciones a realizar para gestionar el incidente.
- Salida: Resultado de las acciones realizadas producto de la gestión del incidente.

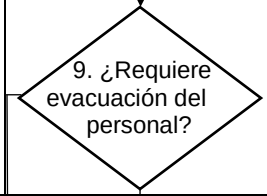
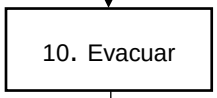
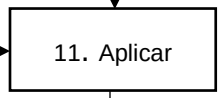
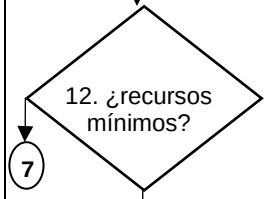
Cuadro 67. Desarrollo del plan de contingencia

Fase	Actividad	Descripción	Responsable	Entrada	Salida
-	Inicio	-	-	-	-
Detectar	1. Detectar incidente	Registrar y/o reportar incidencia al líder del servicio TI, mediante los canales de comunicación definidos por Grow Data.	Grupo de Monitoreo	-	Correo electrónico Llamada telefónica
Detectar	2. Analizar incidente	Recibir y analizar el incidente reportado por el grupo de monitoreo	Líder del servicio	Correo electrónico Llamada telefónica	-
Diagnosticar	3. Evaluar incidente	Evaluar y diagnosticar el origen que genera la incidencia sobre el servicio TI y sus posibles soluciones	Líder del servicio	Correo electrónico Llamada telefónica	-
Diagnosticar	4. ¿Es un evento catastrófico? 3	Validar si la incidencia es catastrófica para los servicios TI. SI: Se continua a la actividad No. (5) NO: Se continua a la actividad No. (3)	Líder del servicio	-	Resultado Decisión
-	A	-	-	-	-

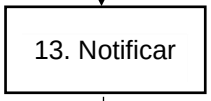
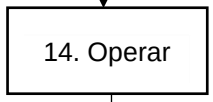
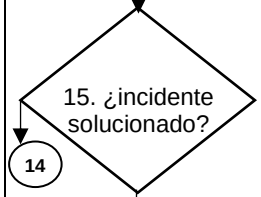
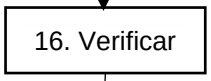
Cuadro 67. (Continuación)

Fase	Actividad	Descripción	Responsable	Entrada	Salida
-	A	-	-	-	-
Diagnosticar	5. Convocar	Convocar al Equipo de recuperación	Líder del servicio	-	Llamada telefónica
Diagnosticar	6. Diagnosticar	Diagnosticar evento catastrófico	Equipo de recuperación	Correo electrónico Llamada telefónica	-
Diagnosticar	7. ¿Activar Plan de contingencia? 3	Tomar la decisión de activar o no el plan de contingencia del servicio TI, de acuerdo con el diagnóstico realizado a la incidencia y a los criterios de activación. SI: Se continua a la actividad No. (8) NO: Se continua a la actividad No. (3)	Líder de Equipo de recuperación	-	Resultado Decisión
Activar	8. Activar	Activar el plan de contingencia del servicio TI “Control de Acceso”	Líder del Equipo de recuperación	Llamada telefónica	-
-	B	-	-	-	-

Cuadro 67. (Continuación)

Fase	Actividad	Descripción	Responsable	Entrada	Salida
-		-	-	-	-
Activar		Evaluar si es necesaria la evacuación del personal que puede verse afectado por la catástrofe. Si: Se pasa a la actividad no. (10) No: Se pasa a la actividad no (11)	Líder del Equipo de recuperación	-	Resultado Decisión
Activar		Autorizar la evacuación del personal que se puede ver afectado durante el evento catastrófico	Equipo de recuperación	-	Llamada telefónica
Activar		Activar plan de contingencia del servicio (diagnóstico de soporte en sitio, desplazamiento de personal técnico a las sedes, etc.)	Equipo de recuperación	Plan de Contingencia para el servicio TI “Control de acceso”	Llamada telefónica
Activar		Validar si se cuentan con los recursos mínimos para entrar en contingencia. SI: Se pasa a la actividad no. (13) No: Se pasa a la actividad no. (7)	Líder del Equipo de recuperación -	-	Resultado Decisión
-		-	-	-	-

Cuadro 67. (Continuación)

Fase	Actividad	Descripción	Responsable	Entrada	Salida
-		-	-	-	-
Operación en contingencia		El equipo de comunicación notifica a las partes interesadas el inicio de la operación en contingencia.	Equipo de comunicación	-	Llamada Telefónica
Operación en contingencia		Se opera siguiendo las estrategias establecidas en el plan de contingencia del servicio TI “Control de acceso”	Equipo de recuperación	Plan de Contingencia para el servicio TI “Control de acceso”	-
Operación en contingencia		Evaluar si ya fue solucionado el incidente catastrófico. Si: Se pasa a la actividad no. (16) No: Se pasa a la actividad no. (14)	Líder del Equipo de recuperación	-	Resultado Decisión
Operación en contingencia		Verificar la disponibilidad del servicio TI “Control de acceso”	Equipo de recuperación	Llamada Telefónica	-
-		-	-	-	-

Cuadro 67. (Continuación)

Fase	Actividad	Descripción	Responsable	Entrada	Salida
-	D	-	-	-	-
Operación en contingencia	17. ¿retorno a normalidad? 14	Validar si se puede volver a la operación normal teniendo en cuenta los criterios de vuelta a la normalidad. SI: Se pasa a la actividad no. (18) NO: Se pasa a la actividad no. (14)	Líder del Equipo de recuperación	-	Resultado Decisión
Operación en contingencia	18. Consolidar	Consolidar los registros de la información procesada durante la operación en contingencia	Equipo de recuperación	Datos procesados durante la operación en contingencia	-
Vuelta a la normalidad	19. Comunicar	Comunicar a las partes interesadas el regreso de la operación en normalidad	Equipo de comunicaciones	-	Llamada Telefónica
Vuelta a la normalidad	20. Generar	Generar el informe del manejo de la crisis	Líder del Equipo	-	Informe manejo de crisis
-	E	-	-	-	-

Cuadro 67. (Continuación)

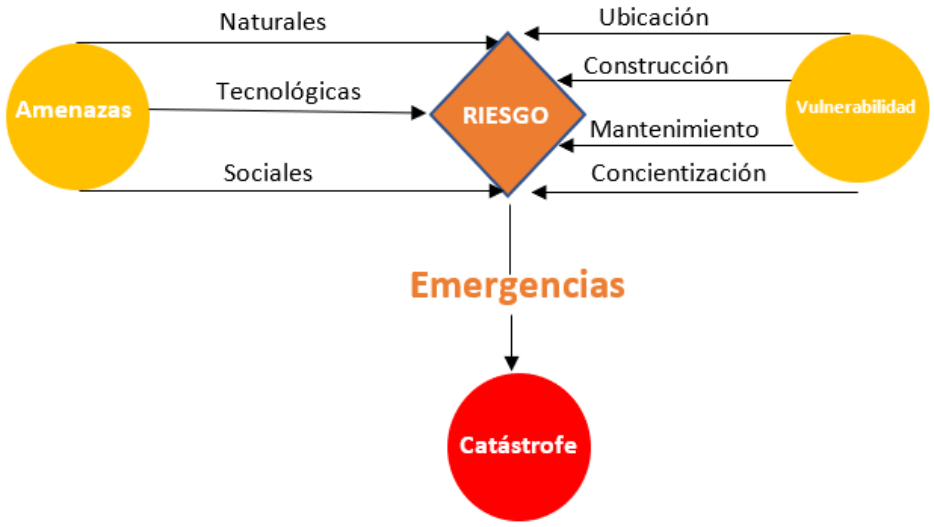
Fase	Actividad	Descripción	Responsable	Entrada	Salida
-	E	-	-	-	-
Vuelta a la normalidad	21. Valorar	Valorar los daños presentados por el evento catastrófico.	Equipo de recuperación	Informe manejo de crisis	-
Lecciones aprendidas	22. Generar	Generar informe de mejoramiento (qué se hizo bien, qué se hizo mal, qué se pudo evitar, recomendaciones, etc.)	Líder Equipo	-	Informe de mejoramiento
-	Fin	-	-	-	-

Fuente: Elaboración propia

5.16 IDENTIFICACIÓN ESCENARIOS DE AMENAZAS

Actualmente el servicio TI “Control de acceso” también se encuentra expuesto a sufrir afectaciones en su continuidad debido a múltiples escenarios de amenazas que no están ligados directamente a los activos de información identificados en este documento, sin embargo Grow Data debe comprender aquellos conceptos, escenarios y su estrecha relación entre sí, para lograr identificar de una manera acertada aquellos riesgos de continuidad a los cuales la organización está expuesta a una afectación directa a la prestación del servicio TI “Control de acceso”, en la siguiente figura 5 se describe la relación de los riesgos:

Figura 5. Riesgos de Continuidad



Fuente: Elaboración propia

- Amenazas: Evento que tiene la propiedad potencial de dañar activos relacionados con el servicio TI “Control de acceso” ofrecido por Grow Data tales como información biométrica, procesos de registro y control, sistemas de información, personas y por lo tanto causar daño a la Entidad. Estas se pueden clasificar en:
- Naturales: Aquellos elementos del medio ambiente que son peligrosos al personal y servicio TI “Control de acceso” ofrecido por Grow Data, que están causados por fuerzas ajenas a él.
- Tecnológicas: Las amenazas tecnológicas o cibernéticas pueden interrumpir operaciones del servicio TI “Control de acceso” ofrecido por Grow Data, generando multas, demandas causando impactos financieros y de reputación.

- Sociales: producidas por cambios en la dinámica social producto de afectaciones de sus derechos y entrega de servicios públicos, generando indisponibilidad en las operaciones del servicio TI “Control de acceso”.
- Vulnerabilidad: Situación que facilita que una amenaza explote una vulnerabilidad causando daño a los activos tales como información, procesos, sistemas, personas y por lo tanto causar daño a la Entidad. Estas se pueden clasificar en:
- Ubicación: Estas se enfocan en la localización del edificio de la operación principal de la entidad que Grow Data preste el servicio TI “Control de acceso”.
- Construcción: Estas se enfocan en la estructura del edificio de la operación principal de la entidad que Grow Data preste el servicio TI “Control de acceso”.
- Mantenimiento: Estas se enfocan en el mantenimiento a la infraestructura del edificio de la operación principal de la entidad que Grow Data preste el servicio TI “Control de acceso”.
- Concientización: Estas se enfocan en la falta de cultura organizacional, en el uso y apropiación al interior de la entidad, sentido de pertenencia por parte de los grupos de interés y de valor.

Igualmente es importante identificar tanto los factores internos como externos que pueden afectar la entrega del servicio TI, ya que esto permite tener una visión más completa de los riesgos asociados a la continuidad del negocio. Los factores internos son aquellos que se originan dentro de la organización, como la infraestructura tecnológica, los recursos humanos, la gestión de procesos, entre otros. Por otro lado, los factores externos son aquellos que provienen del entorno de la organización, como eventos naturales, fallas en los servicios públicos, cambios en la regulación gubernamental, entre otros. Al identificar y clasificar estos factores, se pueden establecer medidas preventivas y de contingencia para minimizar los impactos negativos en la entrega del servicio TI., en el cuadro 68 se detallan estos factores:

Cuadro 68. Clasificación de los escenarios de amenaza

Categoría	Factores	Escenarios
Interno	Colapso de Infraestructura física: Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor.	Error de Hardware
		Incendios
		Sismos
		Inundaciones
Externo	Desastre Tecnológico: Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos.	Ciberataques
		Fallas en fluido eléctrico.
	Emergencia social: Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.	Movilizaciones
		Ataques terroristas

Cuadro 68. (Continuación)

Categoría	Factores	Escenarios
Externo	Pandemia: Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.	Pandemia
Fuente: Elaboración propia		

- Error de Hardware**:** Se identifican por presentar comportamientos anómalos en las partes que conforman los equipos informáticos, los más comunes son: fallas en el microprocesador, errores en la CPU, errores en la tarjeta gráfica, errores en la fuente de alimentación y errores en la memoria RAM. Teniendo en cuenta las fallas anteriormente presentadas son muy comunes en la dinámica normal de Grow Data en el servicio TI "Control de acceso".
- Incendios: Un incendio es un evento de fuego no controlado, en el cual se pueden afectar personas y estructuras físicas produciendo daños de gran impacto (lesiones leves, lesiones graves o lesiones mortales). Por lo general son generados por humanos de carácter intencional o no intencional. Por todo lo anterior las organizaciones no están exentas de sufrir algún foco de incendio en la infraestructura, por ende, pueden ser afectadas vidas humanas y activos de Grow Data en el servicio TI "Control de acceso".
- Sismos: Es una liberación de energía que se produce por el desplazamiento brusco y repentino entre dos placas tectónicas o por el movimiento repentino en una falla geológica**,** todo lo anterior se produce de forma natural por ende Grow Data se vería afectada directamente teniendo afectaciones en su infraestructura hasta pérdidas humanas.
- Inundaciones: Es el exceso de agua, invadiendo áreas que en condiciones normales están secas. Se identifican una serie de principales causas en donde se encuentran las siguientes: lluvias frecuentes e intensas, rompimiento de tuberías, falta de capacidad hidráulica de las redes de alcantarillado, taponamiento de sumideros y tuberías, todo lo anterior se produce de forma natural o alterada por el hombre por ende Grow Data se vería afectada directamente teniendo daños en su infraestructura hasta pérdidas humanas.
- Ciberataques: Ataque dirigido contra el sistema informático de una organización. En los últimos años de manera simultánea al desarrollo y uso de nuevas tecnologías se ha experimentado un crecimiento de diferentes técnicas y tácticas en la ejecución de los ciberataques generando pérdidas millonarias, es así como no solamente las pérdidas económicas generarían una entropía si no, interrupciones en el servicio TI "Control de acceso"., además la perdida de reputación y afectaciones legales podrían materializarse.
- Fallas en el fluido eléctrico: Para Grow Data la no prestación de su servicio TI "Control de acceso" debido a fallas relacionadas con el fluido eléctrico se vería altamente afectado, desencadenando que los objetivos misionales y estratégicos de la organización no se puedan alcanzar.

- Movilizaciones: demandas realizadas por numerosas personas que se pueden llegar a sentir perjudicadas por diversas razones (mala prestación de un servicio público, violación de sus derechos, etc.) y que realizan una movilización buscando respuestas a sus demandas y encontrar soluciones. El conflicto debe ser adecuadamente canalizado y gestionado para evitar que la protesta se transforme en violencia. En estos casos se pueden ver afectadas la prestación del servicio TI “Control de acceso” de Grow Data.
- Ataques terroristas: A nivel de orden público en la sociedad colombiana es una de las actividades que han marcado la historia del país, en donde se ve afectada la población en gran medida buscando daños en la infraestructura de las ciudades.
- Pandemia: Teniendo en cuenta que en los dos últimos años en Colombia y el mundo se está viviendo el contagio de una enfermedad epidémica que se extiende a varios territorios afectado a la mayoría de su población, además que la lentitud en el dimensionamiento de la magnitud evidencia la falta de preparación para los diferentes efectos que esta produce. La afectación pasa por afectación en la prestación del servicio hasta pérdidas humanas.

5.17 ESTRATEGIAS DE CONTINUIDAD ESCENARIOS DE AMENAZA

Después de tener identificados los diferentes escenarios de amenaza y los factores internos y externos, a continuación, se establecen las diferentes estrategias que Grow Data debe seguir para poder asegurar la continuidad en la prestación del servicio TI “control de acceso”.

5.17.1 Ciberataques. Los ciberataques constituyen uno de los principales escenarios de amenazas que puede afectar a la continuidad del negocio en las diferentes entidades y organizaciones a nivel nacional. Por lo anterior, Grow Data debe asignar los recursos necesarios para proteger la información crítica evitando afectar la entrega del servicio TI “Control de acceso”.

A continuación, se enlista la estrategia de continuidad para el escenario de amenaza de ciberataque:

- Buscar que los programas, proyectos y campañas de concientización y sensibilización, así como las capacitaciones que adelante en la entidad a la cual se le presta el servicio TI “Control de acceso”, se tenga en cuenta al personal de Grow Data alineándose con las políticas para la seguridad de la información.
- Identificar y actualizar los activos asociados al servicio TI “Control de acceso” y las instalaciones de procesamiento de información, ayudando a asegurar que se cuenta con una protección efectiva.
- Clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Implementar procedimientos para la gestión de medios de almacenamiento removibles alineados con las políticas adoptadas por la organización.
- Restringir al acceso de la información a los usuarios, brindando menús para controlar el acceso a las funciones de los sistemas a las aplicaciones.
- Uso de formularios de autenticación para el acceso de información o aplicaciones de sistemas críticos.
- Alinear con la política de seguridad que prohíba el uso de software no autorizado, realizar un listado de listas blancas y negras de las aplicaciones.
- Alinear con la política de seguridad de la entidad para la prestación del servicio TI “Control de acceso” protegiendo los activos de a cargo contra riesgos con la obtención de archivos y de software mediante redes externas o cualquier otro medio.
- Instalar y actualizar el software de detección y reparación del software malicioso en los computadores asignados para la prestación del servicio TI “Control de acceso” en forma rutinaria.
- Alinearse con las políticas de copias de respaldo de la información, del software imágenes de los sistemas, además aplicarle las pruebas de restauración.

- Alinear los activos y aplicativos para el registro y seguimiento de eventos para evaluar las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Establecer procesos y procedimientos para supervisar, estudiar y poner en marcha las respuestas a los incidentes y alertas de seguridad. Las posibles respuestas pueden incluir: aumentar la vigilancia, aislar el sistema, aplicar parches, etc.
- Ejecutar análisis forense digital en caso de ser necesario, preservando la cadena de custodia.
- Ejecutar el plan de contingencia del servicio TI “Control de acceso” durante y después de un incidente cibernético.
- Fortalecimiento y mayor capacidad tecnológica de los organismos de seguridad para la inspección de la red.
- Campañas de comunicación en ciberseguridad para la prevención y mitigación de posibles fraudes (políticas de seguridad de la información, antivirus, paredes de fuego, sistemas de detección de intrusos).
- Campañas pedagógicas dirigidas a los funcionarios de Grow Data y orientadas a reconocer las modalidades más utilizadas por los ciberdelincuentes (phishing, skimming, programa maligno, entre otros).
- Gobernanza de la identidad estableciendo Políticas acerca de quien tiene acceso a aplicaciones y recursos al interior de Grow Data esencialmente aplicado a los usuarios privilegiados.
- Verificación de las políticas por parte de los diferentes administradores que supervisan el acceso a estos aplicativos y recursos asegurando su revisión y actualización.
- Establecer controles específicos, especialmente para los usuarios privilegiados identificando los límites que pueden hacer, cuando y donde.
- Verificación de controles específicos de seguridad como los respaldos o copias de seguridad de la información, listas de control de acceso de manera periódica.
- Configurar los sistemas operativos de forma segura.
- Implementar mecanismos de bloqueo de los dispositivos.
- Implementar el filtrado del tráfico de la red en dispositivos de usuario final.
- Control de dispositivos extraíbles tales como pendrive, discos duros externos, tarjetas de memoria, discos ópticos.
- Contar con pólizas de seguros que ayuden a Grow Data frente a incidentes derivados de las amenazas cibernéticas.
- Coordinar al equipo de trabajo que hará frente al ciberataque, definiendo roles, responsabilidades y límites.
- Monitorear continuamente las actividades realizadas que buscan mitigar el ataque.
- Gestionar la configuración de la red de forma segura, garantizando que los usuarios puedan acceder a los servicios para los que hayan sido autorizados específicamente.

- Documentar el alcance del ataque para identificar cuando empezó, que datos y sistemas fueron comprometidos. Todo esto para dejar una trazabilidad en la investigación y mantener información de lecciones aprendidas para próximos incidentes.
- Coordinar con el área jurídica de la entidad para evaluar las posibles responsabilidades generadas por el ciberataque.
- Revisión, auditoría y monitoreo de la eficiencia de los controles de seguridad

5.17.2 Movilizaciones. En los últimos años el país ha sido testigo del incremento de las protestas o movilizaciones sociales generadas por el descontento de la sociedad frente a las diferentes políticas derivadas por la gestión de sus gobernantes, generando caos en la seguridad de las personas y en la movilidad al interior de las ciudades.

En la ciudad de Bogotá estas manifestaciones han presentado una mayor relevancia debido a que en la ciudad se concentra el poder gubernamental derivando en afectaciones de la operación de sus diferentes entidades y organizaciones privadas.

Grow Data no es ajeno a estas situaciones por lo tanto debe definir la estrategia para garantizar la continuidad de la prestación de servicio TI “Control de acceso” cuando sus colaboradores no puedan ingresar al edificio de la entidad a la cual se le está prestando el servicio, debido a la afectación del orden público, caos en el sistema de transporte, vandalismo, etc.

A continuación, se enlista la estrategia de continuidad para el escenario de amenaza de movilizaciones:

- Evitar confrontaciones con los manifestantes evitando que se presente afectación en la integridad física de los funcionarios de Grow Data, capacitaciones sobre resolución de conflictos.
- Identificar salidas alternas en las instalaciones donde se esté prestando el servicio TI para evacuar a los funcionarios de Grow Data en caso de ser necesario.
- Asegurar la evacuación de los funcionarios de Grow Data del edificio donde se esté prestando el servicio en caso de ser necesario.
- Documentar e identificar a los colaboradores que por su perfil es necesario habilitar el acceso remoto a los recursos y a los sistemas necesarios para asegurar la continuidad de la prestación del servicio.
- Habilitar el acceso remoto a los recursos y sistemas de Grow Data a los colaboradores previamente identificados.

5.17.3 Terrorismo. Este es uno de los flagelos a nivel de orden público que más ha afectado a la sociedad colombiana a través de la historia, afectando en gran medida a la población civil y buscando causar daños en la infraestructura de las ciudades.

Muchos de los ataques terroristas van enfocados en causar el mayor daño posible a las instituciones gubernamentales y de seguridad. Grow Data identifica a los ataques terroristas como un factor que puede afectar la continuidad de sus operaciones, por lo tanto, es necesario contar con la estrategia adecuada para asegurar la continuidad de la prestación de servicio TI “Control de acceso”.

A continuación, se enlista la estrategia de continuidad para el escenario de evento de Terrorismo:

- Identificar salidas alternas en las instalaciones donde se esté prestando el servicio TI para evacuar a los funcionarios de Grow Data en caso de ser necesario.
- Asegurar la evacuación de los funcionarios de Grow Data de las instalaciones donde se esté prestando el servicio TI.
- Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían tener personas que puedan respaldarlos en caso de que resultado del incidente de incendio no puedan ejercer sus responsabilidades, afectando la continuidad de la prestación del servicio TI.
- Activar a aquellos colaboradores que sean respaldo de personal clave dentro de Grow Data, en caso de que no puedan ejercer sus responsabilidades
- Habilitar el acceso remoto a los recursos y sistemas para la operación normal de los empleados de Grow Data.

5.17.4 Fallas eléctricas. Para la consecución del alcance de los objetivos de Grow Data es indispensable ofrecer las condiciones de trabajo optimas teniendo en cuenta lo anterior las fallas eléctricas es un factor importante para que los diferentes actores puedan cumplir con sus compromisos así cumplir con las metas establecidas.

El fluido eléctrico es un factor importante para la operación del servicio TI “Control de acceso” por lo tanto, a continuación, se enlista la estrategia de continuidad para el escenario de fallas del fluido eléctrico:

- Gestionar el uso de plantas eléctricas que suplan la falta de energía en la organización que Grow Data este prestando el servicio.
- Realizar adquisición de equipos que protejan contra fluctuación de la energía eléctrica.

- Gestionar el acceso y control remoto, estableciendo el acceso seguro, evitando el uso indebido de los activos de Grow Data.
- Realizar mantenimiento de los equipos a cargo de Grow Data, para asegurar su disponibilidad e integridad continua.

5.17.5 Sismo. Para Grow Data la preparación para afrontar las consecuencias de un sismo es muy importante debido al servicio T.I. prestado en caso de materializarse el evento[30].

Es un factor que puede afectar la continuidad del servicio T.I. por lo tanto, es necesario contar con una estrategia adecuada para asegurar el funcionamiento es así como a continuación se enlista la estrategia de continuidad para el escenario de sismo:

- Identificar salidas alternas en las instalaciones donde se esté prestando el servicio TI “Control de acceso” para evacuar a los funcionarios de Grow Data en caso de ser necesario.
- Asegurar la evacuación de los funcionarios de Grow Data de las instalaciones donde se esté prestando el servicio TI “Control de acceso”.
- Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían tener personas que puedan respaldarlos en caso de que resultado de las acciones terroristas no puedan ejercer sus responsabilidades, afectando la continuidad de la prestación del servicio TI “Control de acceso”.
- Gestionar la consulta de la información respaldada según las políticas de back up, asegurando su disponibilidad en caso de ser requerida.

5.17.6 Inundación. Para Grow Data la preparación para afrontar las consecuencias de una inundación es muy importante debido al servicio TI “Control de acceso” prestado en caso de materializarse el evento. Desde desbordamiento de ríos, alcantarillas bloqueadas, hasta lluvias excesivas[31].

A continuación, se enlista la estrategia de continuidad para el evento de Inundación:

- Identificar salidas alternas en las instalaciones donde se esté prestando el servicio TI para evacuar a los funcionarios de Grow Data en caso de ser necesario.

[30] INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO. Caracterización General del Escenario de Riesgo Sísmico. Obtenido de: https://www.idiger.gov.co/rsismico el 30 de marzo de 2021.
[31] INSTITUTO DISTRITAL DE GESTIÓN DE RIESGO Y CAMBIO CLIMÁTICO. Caracterización General del Escenario. Obtenido de: https://www.idiger.gov.co/rinundacion el 29 de marzo de 2021.

- Asegurar la evacuación de los funcionarios de Grow Data de las instalaciones donde se esté prestando el servicio TI “Control de acceso”.
- Identificar y documentar a aquellos colaboradores que por sus roles y responsabilidades deberían tener personas que puedan respaldarlos en caso de que resultado de las acciones terroristas no puedan ejercer sus responsabilidades, afectando la continuidad de la prestación del servicio TI “Control de acceso”.
- Activar a aquellos colaboradores que sean respaldo de personal clave dentro de Grow Data, en caso de que no puedan ejercer sus responsabilidades.
- Valoración de los activos afectados tras la materialización del riesgo generando la indisponibilidad y no operación de estos.
- Habilitar el acceso remoto a los recursos y sistemas para la operación normal de los empleados de Grow Data.
- Gestionar la consulta de la información respaldada según las políticas de back up, asegurando su disponibilidad en caso de ser requerida.

5.17.7 Pandemia. Tomando en cuenta el momento actual que se encuentra viviendo el país, donde la incertidumbre de que hacer para afrontar la pandemia aumenta con el paso del tiempo, y al no vislumbrar una solución definitiva a corto y mediano plazo, Grow Data no es ajeno a verse afectado por esta situación. Por lo tanto, documenta la estrategia que se debe seguir para poder asegurar la continuidad del servicio TI “Control de acceso” y poder operar en medio de la actual pandemia del covid-19 teniendo en cuenta la resolución 666 del 24 de abril del 2020 emitida por el Ministerio de Salud y Protección Social y según el decreto 491 del 28 de marzo del 2020.

A continuación, se enlista la estrategia de continuidad para el escenario de amenaza de pandemia:

- Definir los elementos de protección personal y proveerlos a todos los funcionarios de Grow Data que excepcionalmente deban asistir a las instalaciones de la entidad a la cual se le presta el servicio TI “Control de acceso”.
- Desarrollar e implementar un protocolo de limpieza y desinfección permanente del lugar de trabajo, con base en las características establecidas en el protocolo de bioseguridad, incrementando la frecuencia de limpieza y desinfección tanto de las áreas comunes como de los puestos de trabajo que estén siendo ocupados.
- Limitar las reuniones y eventos presenciales, salvo en casos excepcionales, en los cuales se deberá restringir el número de asistentes y tiempo de la reunión, así como garantizar la distancia mínima entre los participantes y las medidas de limpieza y desinfección establecidas en el protocolo de bioseguridad. En todo caso se deberá dar prioridad a las reuniones y eventos virtuales.

- Incentivar el uso de medios de transporte alternativos e individuales como la bicicleta, motocicleta o vehículo propio para el desplazamiento al lugar del trabajo.
- Establecer las medidas de coordinación con las Administradoras de Riesgos Laborales, que aseguren la asesoría y acompañamiento continuo para atender las necesidades del control de riesgo laboral por Covid-19.
- Los funcionarios deben lavarse las manos constantemente al llegar a las instalaciones de la entidad a la cual se le esté prestando el servicio TI y al salir de ellas.
- El uso del tapabocas es obligatorio mientras se encuentre al interior de las instalaciones de la entidad a la cual se le esté prestando el servicio TI.
- Respetar la distancia mínima de seguridad (2 metros) en cualquier parte de la entidad a la cual se le esté prestando el servicio TI.
- Determinar los impactos que tendrían las diferentes medidas de control emitidas por organismos oficiales de salud (Ministerio de Salud y Protección Social).
- Establecimiento de equipos para la toma de decisiones de emergencia, o equipo de respuesta a emergencias, en donde se establezca la estrategia y marque los objetivos del plan de emergencia donde se garantiza la inmediatez y precisión en la toma de la decisión.

6. CONCLUSIONES

- En este proyecto de grado se diseñó un plan de contingencia para el servicio TI "Control de Acceso" ofrecido por Grow Data. Lo más importante del diseño del plan de contingencia es que Grow Data identifica su nivel de desempeño en cuanto al restablecimiento del servicio TI, lo que permite que la empresa mantenga su compromiso de ofrecer un servicio confiable a sus clientes y ayuda a minimizar el impacto financiero y de reputación que una interrupción del servicio podría causar.

- Al identificar y valorar los activos de información relacionados al servicio TI, se estableció la importancia que tiene para Grow Data tener la capacidad de gestionarlos de una manera eficiente al identificar su nivel de confidencialidad, integridad y disponibilidad.

- El análisis de riesgos permitió a Grow Data a identificar amenazas que no se habían mapeado previamente debido a la naturaleza tecnológica del servicio. Por ejemplo, acciones humanas como sabotaje o incumplimientos de contratistas pueden representar riesgos adicionales que se deben tener en cuenta en el análisis de riesgos.

- Grow Data identificó la importancia de la gestión de riesgos en la entrega del servicio TI "Control de acceso", ya que esto no solo puede mejorar la calidad del servicio y la satisfacción del cliente, sino que también puede ser un factor clave para diferenciarse de la competencia y atraer a nuevos clientes.

- La documentación de los tratamientos de riesgos es una herramienta valiosa para demostrar a los clientes potenciales que Grow Data toma en serio la seguridad y la continuidad del servicio, y que ha implementado medidas efectivas para mitigar los riesgos asociados con el control de acceso. Esto puede generar una mayor confianza en los clientes actuales y potenciales, lo que a su vez puede contribuir a aumentar la reputación y la proyección del servicio TI ofrecido por Grow Data.

- Grow Data dimensionó los impactos negativos que podrían causar la falta de operación del servicio TI, además de priorizar procesos y reducir costos. Gracias a esto, la empresa puede planificar y prepararse adecuadamente para cualquier evento adverso que pueda afectar el negocio.

- Para Grow Data el diseño estructurado del plan de contingencia y la documentación de los pasos lógicos para su activación son fundamentales para garantizar una respuesta rápida y efectiva ante una crisis en la operación del servicio TI.

- Grow Data obtiene una visión amplia y actualizada de los escenarios de amenaza que puedan afectar su servicio TI, ya que esto permite tomar medidas preventivas y de mitigación de riesgos para reducir la posibilidad de interrupciones y mejorar la continuidad del negocio.

- Durante el presente proyecto se aplicaron los conocimientos adquiridos durante el programa de especialización de seguridad informática, donde se ayudó a Grow Data a mejorar sus procesos, fortaleciendo su gestión en la continuidad del negocio, logrando conectar el conocimiento teórico con el conocimiento práctico, y aplicando lo enseñado en un caso real, alcanzando así una experiencia de fortalecimiento y crecimiento profesional para los autores de este proyecto de grado.

7. RECOMENDACIONES

Se recomienda migrar los aplicativos BMS ARQUERO y Biostar2 a servicios en la nube, ya que estos sistemas de información son responsables de administrar información crítica para el servicio de control de acceso, que abarca desde el registro de cámaras hasta el registro de acceso físico. Al hacerlo, se podrá garantizar una alta disponibilidad, mejoras en el rendimiento y una mayor flexibilidad al momento de requerir un evento de contingencia.

Para ayudar a Grow Data a realizar un seguimiento medido y efectivo de las incidencias presentadas sobre el servicio TI 'Control de Acceso', se recomienda documentar la planificación y preparación adecuada para dar respuestas a los incidentes de seguridad de manera eficaz. De esta manera, se podrán establecer procedimientos claros para cada tipo de incidente, identificar y clasificar los incidentes de seguridad, establecer un equipo de respuesta a incidentes, realizar simulaciones y entrenamientos regulares, y actualizar el plan de gestión de incidentes de manera constante.

Para garantizar una respuesta efectiva en caso de un evento reportado, se recomienda desarrollar un plan de concientización dirigido a todo el personal de Grow Data. Este plan debe abordar los mecanismos y la existencia de la gestión de incidentes, con el objetivo de que los funcionarios estén debidamente informados y preparados para actuar en caso de un incidente de seguridad. Se sugiere que el plan de concientización incluya información sobre los procedimientos de reporte de incidentes, los roles y responsabilidades del equipo de respuesta a incidentes, los criterios de clasificación de incidentes y los tiempos de respuesta esperados. De esta manera, se podrá garantizar una respuesta oportuna y efectiva ante cualquier evento de seguridad en el servicio de TI 'Control de Acceso'.

Para garantizar una gestión efectiva de incidentes de seguridad de la información en el servicio TI 'Control de Acceso', se recomienda establecer una estructura organizacional claramente definida, con roles y responsabilidades desagregados, que permitan una distribución equitativa de las tareas y eviten la sobrecarga de funciones en unos pocos roles. En este sentido, se sugiere identificar y asignar los siguientes roles: responsable de la gestión de incidentes, responsable de comunicaciones, responsable de análisis y resolución, y responsable de documentación y seguimiento. Cada uno de estos roles debe tener tareas y responsabilidades específicas, bien definidas en términos de gestión de incidentes de seguridad de la información. Con esta estructura organizacional, se podrá responder adecuadamente a todos los tipos de incidentes de seguridad conocidos, garantizando una prestación de servicio efectiva y eficiente.

Se recomienda documentar de manera formal y detallada los mantenimientos preventivos y correctivos realizados en los activos de información que soportan el servicio TI "Control de acceso", incluyendo fechas, actividades realizadas y

resultados obtenidos. Además, se deben establecer planes de renovación de estos activos para mantener un adecuado nivel de seguridad y disponibilidad del servicio. Esto permitirá a Grow Data tener un registro actualizado y completo de los mantenimientos realizados, lo que facilitará la identificación y resolución de incidentes de seguridad relacionados con estos activos de información. Además, permitirá tener una mejor planificación y gestión de los recursos necesarios para realizar los mantenimientos preventivos y correctivos de manera oportuna y eficiente.

La implementación de un WAF (Web Application Firewall) para las aplicaciones BMS ARQUERO y Biostar2 ayudaría a proteger los sistemas de información de posibles ataques de seguridad. El WAF se encarga de inspeccionar el tráfico web en busca de amenazas conocidas y desconocidas, identificar patrones de tráfico malicioso y bloquear el acceso no autorizado a los sistemas. De esta forma, se podría prevenir ataques de vulnerabilidades comunes como Cross-site scripting, SQL injection, entre otros. Además, el WAF podría proporcionar una capa adicional de seguridad a los sistemas de información, permitiendo una mejor protección perimetral y mitigando el riesgo de posibles ataques.

La implementación de un WAF no es una solución completa y definitiva para la seguridad de los sistemas de información, pero es un paso importante en la implementación de una estrategia de seguridad integral.

Se recomienda utilizar una herramienta de correlación de eventos para la identificación de eventos relacionados con la seguridad de la información y para poder determinar los incidentes que puedan afectar la continuidad del servicio. Esta herramienta permitiría recolectar información asociada con los eventos de seguridad de información, lo que permitiría atender los incidentes en tiempo real y evitar posibles retrasos en su identificación y resolución.
Se recomienda, por lo tanto, contar con una o más personas de respaldo que puedan respaldar la prestación y contingencia del servicio TI en caso de que sea necesario.

Se sugiere incluir cláusulas en los contratos con los proveedores que apoyan la entrega del servicio TI "Control de acceso", que exijan acciones de continuidad y compromisos de confidencialidad de la información en la prestación del servicio, tanto en la operación normal como en situaciones de contingencia. De esta manera, se podrá garantizar que los proveedores estén comprometidos con la continuidad del servicio y la protección de la información en caso de eventos que puedan afectar la operación del servicio TI.

La implementación de procedimientos y políticas formales para la administración de los respaldos de información permitirá a Grow Data contar con la confianza necesaria para asegurar la disponibilidad de la información en caso de presentarse un evento que afecte la continuidad del servicio TI.

Se recomienda realizar pruebas al presente plan de contingencia por lo menos una vez al año, teniendo en cuenta que las dinámicas de las organizaciones están en constante cambio, por lo tanto, al tener planes de contingencia actualizados y probados se garantiza una efectividad mayor en su aplicación.

Documentar el procedimiento para la ejecución y/o actualización de parches de seguridad es fundamental para garantizar el correcto funcionamiento de los aplicativos involucrados en la prestación del servicio TI “Control de Acceso”. Esto permitirá tener una guía clara y precisa de los pasos a seguir para la instalación de los parches de seguridad en los sistemas y aplicativos, evitando errores y asegurando que se realice de manera efectiva y sin afectar el funcionamiento del servicio, entre los aspectos a considerar en este procedimiento se pueden incluir la identificación de los parches de seguridad necesarios, la definición de un periodo de pruebas antes de su implementación, la elaboración de un plan de contingencia en caso de que ocurra algún problema durante la instalación, y la definición de responsabilidades y roles de los miembros del equipo encargados de la instalación de los parches de seguridad.

Además, es importante destacar que la documentación del procedimiento para la ejecución y/o actualización de parches de seguridad debe ser revisada y actualizada periódicamente para asegurar que se encuentra alineada con las mejores prácticas de seguridad y con los cambios en los sistemas y aplicativos utilizados en la prestación del servicio TI.

Documentar la infraestructura relacionada con el servicio TI Control de Acceso, es de vital importancia para poder asignar los responsables de la operación normal como en contingencia.

De acuerdo con las buenas prácticas para la gestión de los activos de información, se recomienda a Grow Data realizar el inventario de los activos de información relacionados al servicio TI “Control de Acceso” por lo menos una vez al año, permitiendo tener la información de la línea base actualizada y preparada para responder ante riesgos que puedan afectar la disponibilidad de estos activos.

Se recomienda ejecutar los mantenimientos preventivos y correctivos en un periodo de tiempo más corto, idealmente de manera mensual, ya que estas acciones son fundamentales para reducir las posibles fallas de los equipos y asegurar el funcionamiento continuo del servicio TI "Control de Acceso".

Contar con procedimientos basados en la gestión de riesgos permite a Grow Data poder identificar, analizar y cuantificar las probabilidades de ocurrencia y los impactos negativos que se generan de la indisponibilidad del servicio TI “control de acceso”, así como las acciones preventivas y correctivas que deben implementarse para responder ante esta indisponibilidad del servicio TI.

Se recomienda realizar el inventario y análisis de los riesgos de información relacionados con los activos de información al menos una vez al año, lo que permitirá a la organización tener una visión clara de los riesgos a los que está expuesta su información y tomar medidas preventivas y correctivas en consecuencia.

BIBLIOGRAFÍA

BEDÓN, Marcos.; UTRILLA, José.; ORTEGA, Juan. Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Recuperado de http://www.comtel.pe/comtel2012/callforpaper2012/P26C.pdf, 2012.

FERRUZOLA GÓMEZ, Enrique; DUCHIMAZA, Johanna, RAMOS HOLGUÍN, Johanna, ALEJANDRO, María Fernanda. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE Vol. 6, Nº 1, 2019, p.35

GROW DATA. Grow Data misión [en línea]. Obtenido de https://growdata.com.co/nosotros/ el 22 de 11 de 2021.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. ISO:22301. Sistemas de Gestión y Continuidad del Negocio.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27000. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27001. Anexo A Controles de Seguridad, 2013.

INSTITUTO COLOMBIANO DE NORMAS TECNICAS. NTC-ISO/IEC:27002. Controles de Seguridad, 2022.

INSTITUTO DISTRITAL DE GESTIÓN DE RIESGO Y CAMBIO CLIMÁTICO. Obtenido de Caracterización General del Escenario de: https://www.idiger.gov.co/rinundacion el 29 de 3 de 2021.

INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO. Caracterización General del Escenario de Riesgo Sísmico, IDIGER. Obtenido de: https://www.idiger.gov.co/rsismico el 30 de 3 de 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO), ISO 22301:2019, International Organization for Standardization, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). Asociación MERCOSUR de Normalización (AMN), 2009.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC:27031. Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de la información y la comunicación para la continuidad del negocio, 2011.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).NTC-ISO:31000. Gestión del Riesgo. Principios y Directrices. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (INCONTEC), 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (AMN ISO Guía 73. (2013). Gestión del riesgo - Vocabulario. Asociación MERCOSUR de Normalización (AMN). International Organization for Standardization (ISO).

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, 2012.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - MinTic. Guía para realizar el Análisis de Impacto de Negocios BIA, Bogotá: Mintic, 2015.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía para la Gestión y Clasificación de Activos de Información. Bogotá: Mintic, 2020.

NATIONAL SECURITY AGENCY (NSA). Committee on National Security Systems (CNSS).

VERDÚ FERNÁNDEZ, José Ignacio. Plan de contingencia de tecnologías de la información en entornos distribuidos, Tesis de Licenciatura, 2016.