FACULTAD DE POSTGRADOS

MAESTRÍA EN DERECHO DIGITAL E INNOVACIÓN

TÍTULO DE LA INVESTIGACIÓN

Notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA

Profesor

Lorena Naranjo Godoy

Autores

Claudio Cortés Soria

Alexandra Maldonado Navarro

2022

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido el trabajo, "**Notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA**", a través de reuniones periódicas con los estudiantes Claudio Cortés Soria y Alexandra Maldonado Navarro, en el semestre 2022-II, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación."

_____

Prof. Lorena Naranjo Godoy

CC

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Claudio Cortés Soria

CC

_____

Alexandra Maldonado Navarro

CC

AGRADECIMIENTOS

A la coordinadora de la maestría, Doctora Lorena Naranjo por todo su apoyo durante la maestría.

A la compañía Radical Cia Ltda por la colaboración brindada durante esta investigación.

ÍNDICE DE CONTENIDOS

RESUMEN

La entrada en vigencia de la Ley Orgánica de Protección de Datos Personales establece un marco más sólido y coherente para la protección de datos en el Ecuador. El tratamiento del dato personal dentro del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA LTDA tiene diversas finalidades, diferentes volúmenes de información y complejidad. Es por esta razón que dentro de este ensayo académico se identificarán todos los requisitos necesarios para la noticación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía; entendiendo que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, reconocido en nuestra Constitución.

Palabras clave: Seguridad informática, derecho informático, derecho digital, ciberseguridad, protección de datos.

ABSTRACT

The entry into force of the Organic Law for the Protection of Personal Data establishes a more solid and coherent framework for data protection in Ecuador. The processing of personal data within the Security Operation Center of the Company RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA LTDA has various purposes, different volumes of information and complexity. It is for this reason that within this academic essay all the necessary requirements will be identified for the notification of violation of personal data security breaches of the Security Operation Center of the Company; understanding that the protection of natural persons in relation to the processing of personal data is a fundamental right, recognized in our Constitution.

Keywords: Informatics security, informatics law, digital law, cybersecurity, data protection.

1. INTRODUCCIÓN.

1.1.- Contexto del entorno interno de la organización.

RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA constituida en el territorio ecuatoriano hace más de 21 años, se especializa en productos tales como la provisión e instalación de infraestructura tecnológica, soluciones aplicadas, servicios digitales, ciberseguridad y seguridad digital.

La empresa ofrece el servicio de detectar, analizar y prevenir a través del uso de su Centro de Operación de Seguridad (SOC), la supervisión y administración de la seguridad de los sistemas de información a través de herramientas de recogida, correlación de eventos e intervención remota.

Su misión es proveer soluciones tecnológicas confiables con énfasis en la seguridad digital, integrando herramientas innovadoras y recurso humano honesto y altamente calificado, que garantice la operación de los sistemas atendidos.

La visión de Radical formará parte del equipo de líderes que se encamina hacia el futuro de la seguridad digital, enriqueciendo las vidas alrededor del mundo con las tecnologías más innovadoras y personal calificado responsable, para la operación segura de los sistemas de nuestros clientes.

Entre los servicios que presta la empresa está la búsqueda de soluciones tecnológicas para mejorar la productividad de las compañías, a través de una verdadera transformación digital y de uno de sus ejes principales como son la ciberseguridad y seguridad digital, es por esta razón que dentro de los principales productos y servicios están: sistema de detección de brechas de seguridad, análisis del estado actual de seguridad, plan de seguridad de datos personales, monitoreo y visibilidad del comportamiento la red, utilizando mecanismos de inteligencia artificial y machine learning, solución de respuesta autónoma contra amenazas cibernéticas, gestión de Incidentes de seguridad para prevención de fraude.

RADICAL brinda como actividad principal los servicios de Data Center e Infraestructura, Security Center para redes IT y OT, Ciberseguridad en redes SCADA además de Ciberdefensa. Todo esto basado en un equipo de respuesta a incidentes (CERT Radical), un Security Operation Center 24/7 (SOC), Laboratorio de Investigación en Ciberseguridad y Ethical Hacking. Está es una de las razones por las que dentro de los proveedores que forman parte del giro del negocio de RADICAL, están aquellas compañías que le ayudan en la correlación de eventos e intervención remota, proveen de sistemas de cifrado, realizan análisis de comportamiento maliciosos previniendo la ejecución de malware hasta la fuga de la información y controlan la seguridad perimetral para evitar los ataques externos y sobre todo aquellos en los que se busca denegar un servicio.

La estrategia empresarial de RADICAL se funda en la búsqueda de soluciones personalizadas y exclusivas para cada cliente, basadas en la visibilidad continua de todo el ecosistema digital de la organización. RADICAL, en estos veinte y dos años, ha desarrollado un conjunto de capacidades cibernéticas, que la convierten en una empresa pionera en el sector, que no solo previene, detecta, responde y mitiga los ciberataques, sino que lo hace todo a la vez. La compañía cuenta con un sistema de retroalimentación permanente, con un conocimiento profundo e interconectado, creando un ciclo íntegro en el que cada capacidad refuerza y endurece todo el ecosistema de seguridad.

La principal competidora de RADICAL es DELOITTE, dado que esta corporación tiene un enfoque innovador para transformar, modernizar y ejecutar las plataformas tecnológicas existentes, impulsando mejoras de productos y servicios, junto con su capital humano, innovación tecnológica y soluciones cibernéticas brindan, actualmente, ciertos servicios que RADICAL también ofrece con el mismo objetivo de proteger la información y activos digitales.

1.2.- Contexto del entorno externo de la organización.

Dentro del entorno económico el Ecuador, de acuerdo con el Banco Central del Ecuador (BCE), se establece que la suspensión de las actividades productivas

en el país en el segundo trimestre del 2020 el Producto Interno Bruto (PIB) decreció en 12,4% con respecto al período del 2019, la mayor caída trimestral observada desde el 2000. El PIB totalizó USD 15.790 millones en términos constantes y USD 23.550 millones en valores corrientes (Banco Central del Ecuador, 2020).

Cuando analizamos el entorno socio cultural del Ecuador, la UNESCO (2014) reconoce que la implementación participativa de la cultura al PIB es del 4.76%, y que el porcentaje de la población con ocupaciones culturales es del 2.2%, evidenciando que existe un alto nivel de producción nacional. Sin embargo, la participación en actividades culturales fuera del hogar es del 8.4%, requiriendo mayor apoyo para mejorar aún más el consumo interno de bienes y servicios culturales ya que estos son solo del 3.41% del total de los gastos de consumo de los hogares, además de desarrollar todo el potencial de las industrias culturales a nivel nacional.

En el contexto tecnológico señalamos que:

> “Ecuador ha logrado incrementar en un 12% la cantidad de conexiones generadas de parte de usuarios en Google, que cuentan con un promedio de 2 dispositivos para acceder a plataformas y servicios digitales, captando un 20% de crecimiento promedio transaccionado en canales digitales” (Del Álcazar, 2022).

Todos los cambios que se han venido dando desde la pandemia han logrado que los procesos de transformación tecnológica de las empresas se aceleren y como consecuencia de ellos, todos busquen implementar políticas de transformación e innovación digital.

La trasformación digital en Ecuador todavía es incipiente, sin embargo, en el sector financiero, bancario, seguros y salud, se observan avances en el uso de herramientas y sistemas digitales. En la pos pandemia se demuestra que cualquiera puede ser un objetivo atractivo para los ciberdelincuentes, por tanto, es necesario reforzar la ciberseguridad para proteger la información y activos

digitales.

En España, por ejemplo, se ha registrado, según distintos informes y noticias, que el 70% de las pymes españolas han sufrido un ciberataque (Gonzalo, 2021) durante la crisis sanitaria, lo que supone un costo aproximado de 75.000 euros.

Para finalizar es necesario hablar del entorno ambiental, entendiéndose que el desafío más grande del gobierno es la transición ecológica, entendiéndose como un proceso de cambios en los sistemas de producción y consumo para lograr un modelo económico sostenible, cosa que en el Ecuador no ha pasado.

1.3.- Problema de investigación.

Es necesario definir los requisitos que RADICAL debe cumplir para la notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad (SOC) de la Compañía. Para esto se considerará lo dispuesto en la Constitución de la República del Ecuador (2008) y Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento No. 459 (2021), que establece la detección y notificación de violaciones o brechas de seguridad en materia de datos personales, que puedan afectar a la seguridad de datos de carácter personal incorporados a tratamientos que sean responsabilidad de la empresa, independientemente del formato o soporte en el que estén almacenados u organizados.

En este sentido, RADICAL debe cumplir con las obligaciones relativas a la gestión, respuesta y documentación-registro a nivel interno de incidentes de seguridad; y una vez que ha sido detectada la brecha de seguridad, en función de su naturaleza y alcance, la compañía deberá notificar la vulneración de la seguridad de los datos personales a la Autoridad de Protección de Datos Personales y/o a la Agencia de Regulación y Control de las Telecomunicaciones, a más tardar en el término de cinco días después de que haya constancia de ella, ponderando cuando

la brecha de seguridad pueda entrañar un alto riesgo para los derechos y libertades de los titulares del dato, también se deberá comunicar los afectados.

2. REVISIÓN DE LA LITERATURA.

2.1.-Marco Conceptual.

2.1.1.- ¿Qué son incidentes de seguridad?

Según el Real Decreto 3/2010 (actualmente derogado por el Real Decreto 311/2022 (Ministerio de Asuntos Económicos y Transformación Digital, 2022) por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica define a un incidente de seguridad como un "suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información". Se debe agregar que, la Directiva NIS especifica que un incidente es "todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información" (Ministerio de la Presidencia de Gobierno de España, 2010).

Dentro de este trabajo debe quedar claro que un tipo de incidente es la violación de la seguridad de los datos personales siempre y cuando se "destruya, pierda o altere accidental o ilícitamente datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos como reza el artículo 4 apartado 12 del Reglamento 2016/679 del Parlamento Europeo (Parlamento Europeo, 2016).

No obstante, el Grupo de trabajo del artículo 29 (2017), establece la diferencia entre un incidente de seguridad y una violación de la seguridad de los datos personales, determinando que:

> "La consecuencia de tal violación es que el responsable del tratamiento no podrá garantizar el cumplimiento de los principios relativos al tratamiento de los datos personales, tal como se establece en el artículo 5 del RGPD. Esto pone de relieve la diferencia entre un incidente de seguridad y una violación de la seguridad de los datos personales, en esencia, aunque todas las violaciones de la seguridad

de los datos personales son incidentes de seguridad, no todos los incidentes de seguridad son necesariamente violaciones de la seguridad de los datos personales" (Agencia Española de Protección de Datos, 2018).

2.1.2.- ¿Qué son brechas de seguridad?

La Agencia Española de Protección de Datos Personales (AEPD) junto con el RGPD, establecen que una brecha de seguridad es un "incidente de seguridad que afecta a datos de carácter personal", entendiéndose que estas pueden llevarnos a una destrucción, pérdida o alteración de acceso no autorizado de datos personales, independientemente de si es la consecuencia de un accidente o de una acción intencionada afectando tanto a datos digitales como al formato en papel.

Así mismo, se define como brecha de seguridad a las "violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos." (INCIBE, 2020)

Existen múltiples formas en las que se pueden originar estas brechas, especialmente en el entorno digital ya que estas pueden ir desde la destrucción de copias de seguridad, hasta ciberataques de diferentes tipos cuyo objetivo sea acceder a los datos personales almacenados.

Esto quiere decir que, cuando exista una posible vulneración a una brecha de seguridad, el artículo 37 de la Ley Orgánica de Protección de Datos Personales Ecuatoriana, establece que: "El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos".

Por tal razón, el análisis de las brechas de seguridad de RADICAL de los casos de uso del Centro de Operación de Seguridad (SOC) tendrá un componente tecnológico enfocado a los controles y medidas de seguridad y otro que valorará los riesgos para los derechos y libertades de las personas.

2.1.2.- ¿Qué es un Centro de Operación de Seguridad? (SOC)

Cuando hablamos de un centro de operación de seguridad, desde ahora SOC, decimos que se trata de: “un equipo cualificado específicamente en ciberseguridad con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.” (INCIBE, 2020)

Un ataque informático puede ocasionar daños económicos u operativos, como la pérdida de prestigio y reputación. En este sentido, las distintas funciones del SOC de RADICAL están encaminadas a evitar que dichos efectos negativos lleguen a producirse, o incluso se pretende minimizar su riesgo al máximo en caso de que se produzcan.

Puesto que, el SOC de RADICAL, se convierte en un instrumento fundamental para el control a través de la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos que afectan a un proceso particular, también llamado log, esto quiere decir que, RADICAL usa la infraestructura del cliente ya sea el Core bancario, firewall, antivirus, Gestión de Relación con los Clientes (CRM), directorio activo, sistema de planificación de recursos empresariales (ERP) y servidores de aplicaciones varias, para correlacionarlos y mediante casos de uso dar monitoreo y visibilidad al interesado; e incluso llegar a la capacidad de investigación a través de la administración de eventos e información de seguridad (SIEM).

El SOC de la compañía, registra y monitorea de manera exhaustiva todos los sistemas en un período continúo de veinticuatro-siete, arrojando un informe que contiene el análisis de todas las redes, bases de datos o aplicaciones, incluso las detecciones de posibles vulneraciones que puedan comprometer la seguridad del cliente, con el objetivo de tomar las medidas correctivas o de contención anticipadas y oportunas.

Ahora bien, RADICAL al ser responsable de la información que sus clientes envían al SOC, se encargará de identificar en estos casos de uso, si existe o no el tratamiento de un dato personal y sobre ello aplicará la gestión de brechas, el análisis de riesgos y la evaluación de impacto.

3.- GESTIÓN DE BRECHAS DE SEGURIDAD: PREPARACIÓN, DETECCIÓN, IDENTIFICACIÓN Y CLASIFICACIÓN.

El uso de medidas técnicas y organizativas apropiadas por parte de RADICAL, implicará que los datos personales se tratarán de manera que se garantice una seguridad adecuada de los mismos, incluyendo el tratamiento no autorizado, ilícito y contra su pérdida, destrucción o daño accidental como lo establece el principio recogido en el artículo 5, apartado 1, letra f del RGPD.

Ahora bien, RADICAL conoce que cada nivel de respuesta a un incidente de seguridad depende del tamaño de cada cliente, del tipo de dato y del tratamiento que éste tenga, para lo cual llevará una bitácora como responsable de los datos del cliente, para de esta forma se pueda garantizar un nivel de seguridad adecuado al riesgo que implica el tratamiento de los datos personales.

Además, ha establecido la adopción de medidas de protección tecnológicas y organizativas apropiadas para determinar si se ha producido una violación y con ello cumplir la obligación de notificación.

A continuación, se mostrará el proceso de gestión de brechas de seguridad de datos personales que coincide con el proceso de gestión de incidentes:

Figura 1
Procedimiento de gestión de incidentes

Fuente: (Agencia Española de Protección de Datos, 2018).

3.1.-Preparación.

RADICAL identificará un proceso previo de preparación en donde se definirán y decidirán las medidas técnicas y organizativas para afrontar un incidente. En este caso, se designará a los agentes implicados en la gestión de la brecha, el análisis de riesgo y en la evaluación de impacto en el caso de que sea necesario.

La organización cuenta con un plan de respuesta a incidentes de seguridad mismo que contiene un "procedimiento rápido y eficaz para actuar ante cualquier incidente en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro." (INCIBE, 2020)

3.2.- Detección.

En esta fase RADICAL, establecerá lo que es un incidente de seguridad y cuales son las herramientas y mecanismos de detección, que en este caso como responsable tendrá para detectar un incidente, así como, el análisis completo de la información que arrojen todas las herramientas implementadas. Todos estos estos

instrumentos servirán para que la organización identifique una brecha de seguridad y pueda actuar de manera inmediata.

El momento en que se determina la existencia de una brecha de seguridad RADICAL, en armonia a lo que dispone la Ley Orgánica de Protección de Datos Personales del Ecuador identificará al ser responsable del tratamiento del dato personal como y cuando notificar a la autoridad compentente y en algunos casos a los afectados.

Ahora bien, una vez que se ha detectado un incidente de seguridad se debe identificar si fue por fuentes internas o externas a RADICAL.

Lo dicho hasta aquí supone que, fuentes internas son aquellas que la empresa implementará como controles y mecanismos de seguridad dentro y alrededor de las instalaciones, así como de acceso remoto a la información. Estas pueden ser físicas como: el bloqueo de pantallas, accesos con usuarios, cambios constantes de usuarios y contraseñas, entre otros.

RADICAL, cuenta con medios manuales y sistemas automatizados de detección de distinto tipo desde un software antivirus hasta un analizador de logs dentro de su SOC. En este sentido, ante un incidente de seguridad física las repercusiones pueden recaer también en el ámbito de la ciberseguridad y como consecuencia de ello, en el tratamiento del dato personal, por esta razón se coordina siempre entre los responsables de la seguridad fisica y la ciberseguridad.

Por otro lado, las fuentes externas son aquellas que producen una posible detección de incidentes a través de la comunicación de un tercero, esto puede ser proveedores de servicios infromáticos, proveedores de servicios de internet, comunicaciones de organismos públicos, información publicada por un medio de comunicación, entre otros.

3.3.- Identificación y registro.

Una vez que se ha detectado que tipo de fuente de información me puede provocar o no un incidente de seguridad debo identificar la clase, el tipo, la naturaleza, si me afecta o no a un dato de carácter personal y si este puede o no entederse como una brecha de datos de carácter personal midiendo el nivel de riesgo al que se enfrenta RADICAL como responsable del tratamiento del dato personal.

En este sentido, la empresa contará con los medios necesarios para documentar desde el inicio de la detección hasta las medidas de control adoptadas en cada una de las fases de gestión del incidente, sobretodo identificando, si estos incidentes afectaron o no a datos de carácter personal.

3.4.- Clasificación

3.4.1.- Clasificación de incidentes de seguridad.

Una vez que se ha logrado identificar el incidente de seguridad y se ha documentado todos los aspectos del incidente en un registro de incidencias, es importante entender cómo se clasifican estos incidentes de seguridad.

En este caso el Centro Criptológico Nacional de España dentro de su guía de Seguridad de las TICS–CCN-STIC 817 (Centro Criptológico Nacional de España, 2020), establece que para establecer la clasificación de los incidentes de seguridad se debe considerar los siguientes factores:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc.
- Origen de la amenaza: Interna o externa.
- La categoría de seguridad de los sistemas afectados.
- El perfil de los usuarios afectados,
- El número y tipología de los sistemas afectados.
- El impacto que el incidente puede tener en la organización.

- Los requerimientos legales y regulatorio.

Los criterios de clasificación de incidentes de seguridad pueden ser múltiples, los más habituales según INCIBE y ENISA son:

- Incidentes no intencionados o involuntarios;
- Daños físicos;
- Incumplimiento o violación de requisitos y regulaciones legales;
- Fallos en las configuraciones;
- Denegación de servicio;
- Acceso no autorizado, espionaje y robo de información;
- Borrado o pérdida de información;
- Infección por código malicioso.

3.4.2.-Tipos de brecha o violación de la seguridad los datos personales.

Para notificar la violación de datos personales, es necesario remitirnos a los tres principios de seguridad de información que son: confidencialidad, integridad y de disponibilidad.

Brecha o violación de confidencialidad tiene lugar cuando se produce una revelación no autorizada, accidental o con un propósito no legítimo de los datos personales.

Brecha o violación de integridad se entiende como la manipulación, alteración e incluso sustitución no autorizada de los datos personales.

Por último, brecha o violación de disponibilidad, implica la falta de acceso a los datos personales ya sea de manera temporal o definitiva.

Cabe aclarar que, dependiendo las circunstancias, una violación puede afectar a todos al mismo tiempo, así como a cualquier combinación de estos elementos. Incluso si un incidente de seguridad provoca la no disponibilidad de un

dato personal puede convertirse en un tipo de violación ya que la ausencia de acceso a los datos puede recaer sobre derechos y libertades de las personas.

3.4.3.- Valoración del alcance de la brecha o violación de seguridad de los datos personales.

La valoración del alcance de una brecha de seguridad dependerá de como hemos categorizado los datos personales e información tras un incidente de seguridad, ya que de eso dependerá si es que se debe notificar o no al titular o la autoridad competente.

Los efectos adversos pueden depender de algunos factores que se describirán a continuación:

- El nivel de criticidad respecto a la seguridad de los sistemas afectados, que se clasifican en: críticos, muy alto, alto, medio o bajo.
- Las categorias de datos personales afectados según la naturaleza y sensibilidad: los datos de escaso riesgo como son: los de contacto, los de educación; los datos de comportamiento como: localización, hábitos, prefrencias; los datos finacieros y por último los datos sensibles que son aquellos relativos a la vida sexual, salud, entre otros.

Los datos legibles o ilegibles, el volumen de datos personales, facilidad de identificación de individuos, caracteristicas especiales de los individuos, número de individuos afectados, características especiales del responsable del tratamiento, el perfil de los usuarios afectados, el número y tipología de los sistemas afectados, el nivel de impacto que la brecha puede tener en RADICAL desde el punto de vista del tratamiento del dato personal.

La violación de la seguridad de los datos personales puede conducirnos a una serie de efectos adversos que son susceptibles de ocasionar daños y perjuicios a los titulares de ese dato personal. En este sentido, tanto el considerando 85 como el 75 del Reglamento General de Protección de Datos (Parlamento Europeo, 2016)

establecen que estos efectos pueden incluir la pérdida de control sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional. También puede incluir cualquier otro perjuicio económico o social significativo para esas personas.

RADICAL, como responsable del tratamiento de los datos personales debe evaluar si se comunica o no la violación de seguridad de los datos al titular de los mismos, tomando en consideración lo que nos dice el artículo 46 de Ley Orgánica de Protección de Datos Personales (LOPDP, 2021).

4.-CONSECUENCIAS DE LA VIOLACIÓN DE LA SEGURIDAD DE LOS DATOS PERSONALES.

La violación de la seguridad de los datos personales puede traer consigo algunos perjuicios hacia los titulares de los datos personales, estos pueden ser: físicos, materiales, económicos, sociales e incluso pueden incluir con lo menciona el Reglamento General de Protección de Datos (Parlamento Europeo, 2016) en sus considerandos 85 y 75 la pérdida sobre los datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional.

Por lo que, RADICAL en cumplimiento con el artículo 46 de nuestra ley y en concordancia con lo descrito en el considerando 87 del Reglamento General de Protección de Datos (Parlamento Europeo, 2016), aplicando toda la protección tecnológica adecuada y medidas organizativas oportunas, ha podido identificar en su análisis de riesgo y en su evaluación de impacto que se encuentran anexos a este trabajo, si como responsables del tratamiento del dato personal deben o no notificar la violación de seguridad de los datos a la autoridad de control o a los titulares de este derecho.

A continuación, describiremos cuando se debe notificar tanto a la Autoridad de Protección de Datos Personales, así como al titular del dato personal.

4.1.- Notificación a la Autoridad de Protección de Datos Personales.

Como se explicó anteriormente, cuando existe una violación o brecha de seguridad de datos personales el responsable del tratamiento, en este caso RADICAL, deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar como lo establece el artículo 43 de la ley, en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

En este caso cuando RADICAL tenga constancia de una posible violación por cualquier medio, el responsable puede iniciar un breve periodo de investigación para determinar si es que se produjo o no la violación; tomando en consideración que este período debe ser rápido, oportuno y sobretodo que con él se pueda establecer un grado razonable de certeza, para que con ello se pueda realizar una investigación mas exhaustiva.

RADICAL consiente de esta necesidad, ha creado una política de notificaciones de brechas de seguridad con el fin de disponer de un criterio común a todos los tratamientos de datos personales que consten en el registro de actividades de tratamiento del SOC.

Así mismo, la empresa como responsable del tratamiento debe adoptar medidas y mecanismos adecuados para prevenir, reaccionar y ser resilientes ante una violación de seguridad de datos personales; toda esta información se encontrará detallada en el plan de respuesta a incidentes que ayudará al

responsable del tratamiento a “planificar de forma eficaz y a determinar quién, dentro de la organización, tiene la responsabilidad operativa de gestionar una violación y si se debe remitir un incidente a un nivel superior según proceda, así como la manera de hacerlo” (Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, 2017).

4.2.-Notificación al titular de los datos personales.

Por otro lado, nuestra Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) en el artículo 46 establece que:

> “El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo”

Esto quiere decir que, además de notificar a la autoridad de control, el responsable del tratamiento también está obligado a comunicar a las personas afectadas la existencia de una violación de la seguridad, cuando ello implique un riesgo para sus libertades y derechos; esto conllevará una comunicación clara, ágil y en un lenguaje claro y sencillo en donde se describa la “la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación” (Parlamento Europeo, 2016).

Dentro de la guía para la gestión y notificación de brechas de seguridad de la Agencia Española de Protección de Datos personales se establecen factores que se deben tener en consideración para tomar la decisión de realizar la comunicación a las personas afectadas y estas son:

- Cuáles son las obligaciones legales y contractuales.

- Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.
- Existe un riesgo razonable de suplantación de identidad o fraude (en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada).
- Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

La notificacion puede hacerse de forma directa o indirecta, la primera, se entiende por cualquier medio por el cual el responsable se pueda dirigir al afectado ya sea teléfono, correo electrónico, entre otros; mientras que la segunda se usará cuando no sea posible tomar contacto con la persona afectado o cuando la notificación directa represente un costo significativo.

4.3.- Excepciones a la notificación.

Dentro del artículo 46 de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) se establece que no se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas;

2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y,

3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La Autoridad de Protección de Datos, deberá calificar a más tardar en el término de cinco días si cabe o no la excepción de notitifcación de los literales 1 y 2 de este artículo. RADICAL deberá tomar encuenta que la notificación oportuna de la violación de seguridad y la ejecución oportuna de medidas de respuesta siempre serán consideradas como un atenuante ante las infracciones previstas en la ley.

5.- IDENTIFICACIÓN DEL OBJETO DE ESTUDIO.

La presente investigación tiene como objeto central el estudio del noticación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA con sede en la ciudad de Quito. El período temporal que abarcará la investigación corresponde al año 2022.

6.- PLANTEAMIENTO DEL PROBLEMA.

6.1.-Pregunta General de Investigación.

¿Cómo y cuando se debe notificar la violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA LTDA a la Autoridad de Protección de Datos Personales y al titular del dato personal?

6.2.-Efectos del Problema.

La falta de notificación de la violación de brechas de seguridad de datos personales implica que, RADICAL como responsable de los datos personales que se alojan en su SOC, incurriría en una infracción grave.

Además, la sanción económica puede implicar un grave perjuicio para la liquidez de la compañía dado que esta variaria entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa.

Incluso la Autoridad de Protección de Datos Personales va a establecer una multa aplicable en función del principio de proporcionalidad, para lo cual RADICAL tendrá que demostrar que no ha tenido la intención de provocar la brecha de seguridad, que esa conducta no se ha dado de manera reiterativa y que por lo tanto, las consecuencias lesivas y la naturaleza del perjuicio ocasionado para el ejercicio del derecho a la protección de dato no afectan al titular.

Por último, el incumplimiento de la notificación puede provocar la desconfianza de los clientes que tiene RADICAL, perjudicando de manera directa a la imagen y credibilidad que esta compañía ha tenido por 23 años.

6.3.- Causas del Problema.

Las principales causas de que RADICAL no cumpla con la notificación de la violación de brechas de seguridad de datos personales pueden ser el almacenamiento inadecuado de datos personales, una mala práctica en relación con los derechos de acceso, rectificación o cancelación de datos, o cualquier otro incumplimiento de los requisitos establecidos por la ley. Algunas otras causas incluyen la falta de seguridad en la transmisión de datos, el procesamiento de datos sin el consentimiento explícito del titular y el uso indebido de los datos.

En este sentido, como responsable del tratamiento del dato personal se debe realizar uan directriz de notificacion de violacion de brechas de seguridad, instrumento que va a describir y dará cuenta, de modo general, sobre las medidas de seguridad, técnicas, físicas, administrativas y legales que se adopte para garantizar la confidencialidad, integridad y disponibilidad de los datos que maneja dentro de su SOC.

6.4.- Escenarios.

No notificar a la Autoridad de Control de la Ley Orgánica de Datos Personales, Protección de Datos y Privacidad (LOPDP) sobre una brecha de seguridad es una infracción grave de la ley. Esto puede resultar para RADICAL en

sanciones económicas, multas, la cancelación de licencias comerciales y hasta la prohibición temporal de realizar operaciones comerciales. La Autoridad de Control también puede exigir a RADICAL como responsable, la notificación inmediata al titular de los datos afectados por la brecha de seguridad. Además, un tercero afectado por la violación puede presentar una demanda civil para reclamar daños y perjuicios.

7.- OBJETIVO GENERAL.

Diseñar una directriz para la adecuada notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA.

8.- OBJETIVOS ESPECÍFICOS.

1. Identificar cuáles podrían ser las brechas de seguridad de datos personales.
2. Describir la directriz de notificación de violación de brechas de seguridad de datos personales.
3. Determinar cuando se debe notificar a la Autoridad y cuando al titular del dato personal.
4. Establecer un plan de contingencia del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA.

9.- JUSTIFICACIÓN Y APLICACIÓN DE LA METODOLOGÍA.

9.1.- Nivel de estudio.

Este es un proceso descriptivo por que narrará la metodología para la notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA.

9.2.- Modalidad Investigación.

La investigación que se llevará a cabo será la documental y de desarrollo que es una técnica de investigación cualitativa que se encarga de recopilar y seleccionar información a través de la lectura de documentos, libros, revistas, grabaciones, filmaciones, periódicos, bibliografías, etc.

9.3.- Métodos.

Dentro de esta investigación se usará el método inductivo- deductivo, ya que es un procedimiento en el que, comenzando por los datos, se acaba llegando a la teoría. Por tanto, se asciende de lo particular a lo general.

9.4.- Población y muestra.

No es necesario hacer el cálculo de población y muestra ya que es un estudio cualitativo que no exige el uso de un cálculo de una muestra y como es una empresa no necesito un muestreo de la sociedad.

9.5.- Instrumentos de investigación.

Esta investigación realizara un análisis de documentos y entrevistas para recoger información y documentos.

9.6.- Protocolos de investigación.

El presente proyecto se realizará bajo la metodología SCRUM, que es un marco de trabajo liviano que ayuda a las personas, a los equipos y a las organizaciones generar valor a través de soluciones adaptativas para problemas complejos. Para Sonia Mariño y Alonzo Pedro siguiendo a Diaz y Del Dago, nos dicen que el SCRUM, es una colección de procesos para la gestión de proyectos, que permite centrarse en la entrega de valor para el cliente y la potenciación del equipo para lograr la máxima eficiencia, dentro de un esquema de mejora continua (Mariño & Alfonzo, 2014).

Constará de tres fases:

- Planificación
- Desarrollo, y,
- Entrega

9.7 PROPUESTA DE SOLUCIÓN. -

RADICAL, en cumplimiento con la Ley Orgánica de Protección de Datos Personales necesita planificar, identificar, valorar y realizar un análisis de riesgos sobre los derechos y libertades sobre los casos de uso dentro de su Centro de Operación de Seguridad.

Para lograrlo, es necesario plantear y diseñar un formulario donde se evidencie si efectivamente hay una vulneración de una libertad o un derecho y de esta forma RADICAL como responsable de los datos va a notificar a la autoridad y titular cuando y como lo dispone la normativa tomando en consideración la tipología de brecha, tipo de datos y su combinación, tipo de colectivos y el volumen de registros. (ANEXO1)

Así mismo, es importante identificar los riesgos ya sean de identificación electrónica y el riesgo de identificación física, entendiendo que el primero es aquel que hace facilmente identificable al titular del derecho, RADICAL deberá evaluar si públicamente es fácil obtener más información sobre ese conjunto de datos que los hace identificable; y el segundo entendiendo que se puede afectar a las relaciones sociales, evaluando el alto riesgo de afectación a los derechos y libertades del individuo, incluso observando cual es el grado de notoriedad pública de esapersona, entre otras variantes.

RADICAL, cuidará siempre el estado de la información para evitar pérdida de control sobre la misma, evitando el riesgo para los afectados y sobretodo posibles sanciones por vulneración de brechas de seguridad de datos personales.

La organización también ha tomado en consideración que cuando la brecha de datos personales signifique un alto riesgo para los derechos y libertades de los titulares de datos personales,comunicará a los afectados la brecha de seguridad, sin dilación indebida.

RADICAL, en busqueda de una solución ante una posible vulneración de una brecha de seguridad, ha identificado que el ciclo de vida de una brecha no se acaba con el siemple hecho de notificar a la Autoridad de Control y la comunicación a los afectados, es necesario que saque conclusiones, haga seguimiento, corrija errores y elabore un informe final ya que esto le ayudará a prevenir futuros contingentes.

10.- CONCLUSIONES.

1. Se ha considerado que la aplicación del protocolo de gestión de incidentes como uno de los mecanismos necesarios para la consecuencia de objetivos de control específicos de seguridad respecto de la Ley Orgánica de Protección de Datos Personales, donde establece obligaciones a los responsables con relación a la comunicación de las brechas de datos personales a la Autoridad de Control y de la notificación de su ocurrencia a los interesados en función del riesgo para los derechos y libertades que personifiquen, por lo que la gestión de brechas contiene el establecimiento de medidas preventivas y reactivas en función del riesgo inminente pero principalmente en el riesgo residual; es decir, el responsable debe, de forma preventiva, implementar mecanismos de detección y gestión de las brechas.

2. La detección de una brecha no solo supone el empleo de medios técnicos, sino que supone que una información completa sobre las dimensiones e impacto de la brecha llegue a tiempo a los órganos de decisión que deben actuar ante la misma.

3. Con la finalidad de mantener los datos personales seguros y cerciorarse de que nadie tenga acceso a ellos sin autorización, algunas medidas de seguridad simples que se han incluido consisten en almacenar documentos en un gabinete cerrado con llave y poner contraseñas seguras en todos sus dispositivos, mitigando los factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, entre otros.

4. Al manejar un Security Operation Center SOC, los factores de riesgo que se derivan del contexto específico del sector de la actividad, modelo de negocio y al tipo de entidad, son gestionados con los mecanismos de seguridad intrínsecos a la obtención de la información sobre los colectores de LOGs que son un paso previo a la correlación en el SIEM, tales como información cifrada, anonimizada o de componentes netamente técnicos que no permiten coligar datos personales durante la operación y tratamiento de los dato de los clientes.

5. El establecer un proceso descriptivo que narrará la metodología para la notificación de violación de brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA, tanto a la Autoridad competente como al titular, exonerará a la comapañía de posibles sanciones.

11.- RECOMENDACIONES.

1. Es que RADICAL realice un análsiis de riesgos y brecha en donde se priorice el tratamiento a los riesgos de mayor nivel de todos los activos criticos que albergue el SOC.

2. Es importante que RADICAL tome las medidas necesarias dentro del plan de trabajo en donde se defina de mamnera correcta las acciones a implementar una vez que se pueda identifcar violaciones a las brechas de seguridad de datos personales del Centro de Operación de Seguridad de la Compañía.

3. RADICAL debe actualizar y evaluar constantemente los resultados de la implementacion de las medidas de seguridad para de esta forma minimizar sus brechas y con ello la violacion de dato personal de su SOC.

REFERENCIAS

Agencia Española de Protección de Datos. (2018). *Guía para la gestión y notificación de brechas de seguridad.* Ministerio de Defensa. https://www.ucm.es/dpd/file/guiaaepd-quiebras-de-seguridad

Agencia Española de Protección de Datos. (18 de septiembre de 2019). *Brechas de seguridad de datos personales: qué son y cómo actuar*. AEPD: https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar

Asamblea Nacional Constituyente del Ecuador. (2008, octubre 20). Constitución de la República del Ecuador. *Decreto Legislativo 0, Registro Oficial 449, Ultima modificación 25-ene.-2021 Estado: Reformado*. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales.* Registro Oficial No.459, Quinto Suplemento, 26 de Mayo 2021. https://www.consejodecomunicacion.gob.ec/wp-content/uploads/downloads/2021/07/lotaip/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

Banco Central del Ecuador. (30 de Septiembre de 2020). *La Economía Ecuatoriana decreció 12,4% en el Segundo Trimestre de 2020*. BCE:

https://www.bce.fin.ec/index.php/boletines-de-prensa-archivo/item/1383-la-economia-ecuatoriana-decrecio-12-4-en-el-segundo-trimestre-de-2020

Centro Criptológico Nacional de España. (2020). *Guía de Seguridad de las TIC CCN-STIC 817.* Ministerio de Defensa de España. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Del Álcazar, J. (16 de abril de 2022). *Estado Digital Ecuador Abril 2022*. MENTINNO: https://www.mentinno.com/gracias-aqui-esta-tu- informe-estado-digital-ecuador-abril-2022/.

Del Alcazar, J. (s.f.). *Estado Digital Ecuador 2022 - Estadísticas Digitales*. MENTINNO.

European Union Agency For Network And Information Security. (enero de 2016). *ENISA Threat Landscape 2015.* ENISA: https://www.enisa.europa.eu/publications/etl2015/at_download/fullReport

Gonzalo, Á. (21 de julio de 2021). “El 71% de las pymes del país han sufrido un ciberataque durante la pandemia”. *CincoDías (El País Economía)*. CíncoDías : https://cincodias.elpais.com/cincodias/2021/07/21/companias/1626821663_803769.html

Grupo de Trabajo sobre Protección de Datos del Artículo 29 . (2017). *Directrices sobre la notificación de las violaciones de la seguridad de los datos*

personales de acuerdo con el Reglamento 2016/679. Unión Europea. https://www.aepd.es/sites/default/files/2019-09/wp250rev01-es.pdf

IBM. (2022). *Centro de Operaciones de Seguridad (SOC)*. IBM: https://www.ibm.com/mx-es/topics/security-operations-center?mhsrc=ibmsearch_a&mhq=soc

Instituto Nacional de Ciberseguridad de España. (16 de junio de 2014). *¿Qué camino debo seguir para gestionar correctamente un incidente de seguridad en mi empresa?* INCIBE: https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-empresa

Instituto Nacional de Ciberseguridad de España. (12 de diciembre de 2016). *¿Estás preparado para hacer frente a un ciberdelincuente?* INCIBE: https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-ciberincidente

Instituto Nacional de Ciberseguridad de España. (13 de octubre de 2016). *10 «síntomas» de dispositivos tecnológicos «enfermos»*. INCIBE: https://www.incibe.es/protege-tu-empresa/blog/10-sintomas-dispositivos-tecnologicos-enfermos

Instituto Nacional de Ciberseguridad de España. (14 de septiembre de 2016). *Cómo hacer frente a los 5 incidentes de ciberseguridad más comunes (1/2)*. INCIBE: https://www.incibe.es/protege-tu-empresa/blog/hacer-frente-los-5-incidentes-ciberseguridad-mas-comunes-12

Instituto Nacional de Ciberseguridad de España. (19 de septiembre de 2016). *Cómo hacer frente a los 5 incidentes de ciberseguridad más comunes (2/2)*. INCIBE: https://www.incibe.es/protege-tu-empresa/blog/hacer-frente-los-5-incidentes-ciberseguridad-mas-comunes-22

Instituto Nacional de Ciberseguridad de España. (20 de enero de 2016). *Juego de rol. ¿Estás preparado para ser atacado?* INCIBE: https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad

Instituto Nacional de Ciberseguridad de España. (27 de enero de 2016). *Plan de Contingencia y Continuidad de Negocio*. INCIBE: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

Instituto Nacional de Ciberseguridad de España. (11 de abril de 2016). *Políticas de seguridad para la pyme*. INCIBE: https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Instituto Nacional de Ciberseguridad de España. (2016). *Respuesta a incidentes: Políticas de seguridad para la pyme.* INCIBE: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf

Instituto Nacional de Ciberseguridad de España. (11 de abril de 2016). *Taxonomía*. INCIBE: https://www.incibe-cert.es/respuesta-incidentes/rediris/taxonomia

Instituto Nacional de Ciberseguridad de España. (05 de mayo de 2017). *Políticas de seguridad para la pyme: continuidad de negocio.* INCIBE:

https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/continuidad-negocio.pdf

Mariño, S., & Alfonzo, P. (2014). Implementación de SCRUM en el diseño del proyecto del Trabajo Final de Aplicación. *Scientia Et Technica, 19*(4), 413-418. https://doi.org/10.22517/23447214.9021

Martínez, J. (05 de agosto de 2022). *¿Qué es el Centro de Operaciones de Seguridad (SOC) y para qué sirve?* Verne Technology Group: vernegroup.com/actualidad/ciberseguridad/que-es-el-soc-y-para-que-sirve/

Ministerio de Asuntos Económicos y Transformación Digital. (2022). *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.* «BOE» núm. 106, de 04/05/2022. https://www.boe.es/eli/es/rd/2022/05/03/311/con

Ministerio de la Presidencia de Gobierno de España. (2010). *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.* «BOE» núm. 25, de 29/01/2010. https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330&tn=1&p=20220504

Oracle. (2023). *¿Qué es un SOC?* Oracle: https://www.oracle.com/es/database/security/que-es-un-soc.html

Organización de las Naciones Unidas para la Ciencia, la Educación y la Cultura. (2014). *Indicadores UNESCO de Cultura para el Desarrollo. Resumen Analítico Ecuador*. UNESCO: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://en.unesco.org/creativity/sites/creativity/files/cdis/resumen_analitico_ecuador_0_1.pdf

Parlamento Europeo. (2016). *Reglamento General de Protección de Datos.* Bruselas: Reglamento (UE) 2016/679. https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

Universidad de Valencia. (11 de diciembre de 2020). *Noticaciónde Brechas de Seguridad de Datos Personales de la Universität de Valencia.* Universidad de Valencia: https://www.uv.es/lopd/Brechas%20de%20Seguridad/PROTOCOLO%20NOTIFICACION%20BRECHAS%20DE%20SEGURIDAD%20DATOS%20PERSONALES%20UV%20CAS.pdf

ANEXOS

ANEXO1. FORMULARIO DE NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

FORMULARIO DE NOTIFICACIÓN BRECHAS DE SEGURIDAD

1. Datos de la notificación

○ ○ ○

Tipo de notificación: Inicial, Adicional, Completa

Referencia notificación inicial:_____Fecha notificación inicial: _____

2. Identificación del Delegado de Protección de Datos o persona de contacto

Cédula: _____ Nombre: _____

Apellidos: _____ Cargo: _____

Dirección: _____ C.P.: _____

Provincia: _____ Localidad: _____

Teléfono: _____ / _____ e-mail: _____

3. Identificación del responsable del tratamiento

Nombre de la Organización: _____

Tipo de Organización: ◉ Privada, ○ Pública □

RUC:_____Dirección distinta del DPO o persona de contacto:

Dirección: _____ C.P.: _____

Provincia: _____ Localidad: _____

Teléfono: _____ / _____ e-mail: _____

4. Identificación del encargado del tratamiento

¿Hay otra organización implicada en la brecha de seguridad?

Nombre de la Organización:

_____

Tipo de Organización: Privada, Pública

RUC: _____

Dirección: _____ C.P.:

_____

Provincia: _____ Localidad:

_____

Teléfono: _____ / _____ e-mail:

_____

5. Información temporal de la brecha

○ ○

Fecha detección de la brecha:_____ Exacta,

Estimada.

Medios de detección de la brecha:

_____

_____

_____

_____

Justificación de notificación tardía (notificación pasada 72h desde la detección):

Fecha inicio de la brecha: ○ Exacta, □ Estimada.

¿Está resuelta la brecha? Fecha de resolución ○ Exacta, ○ Estimada.

6. Sobre la brecha

Resumen del incidente:

_____

_____

_____

_____

Tipología:

☐ Brecha de confidencialidad (acceso no autorizado)

☐ Brecha de integridad (modificación no autorizada)

☐ Brecha de disponibilidad (desaparición o perdida)

Medio por el que se ha materializado la brecha:

☐ Datos personales

☐ Documentación erdida,

☐ Eliminación incorrecta de

Residuales en

robada o despositada en

datos personales en formato

Dispositivos obsoletos.

Localización insegura

papel.

☐ Hacking

☐ Malware (ejm. Ramsomware)

☐ Phishing.

☐

☐

Correo perdido o abierto. ☐

Dispositivo perdido o robado. ☐

Publicación no intencionada ☐

Datos personales mostrados al individuo incorrecto ☐

Datos personales enviado por error. ☐

Revelación verbal no autorizada de datos personales ☐

Otros:

Contexto

○ Interna (acción no intencionada)

○ Externa (acción no intencionada)

○ Interna (acción intencionada)

○ Externa (acción intencionada)

Otros:

Medidas preventivas aplicadas antes de la brecha:

_____

_____

_____

_____

_____

_____

_____

_____

7. Sobre los datos afectados

Categoría de datos afectados:

☐ Datos básicos ☐ Credenciales de acceso o Identificación ☐ Datos de contacto

☐ Cédula, RUC, ☐ Datos económicos o Financieros. ☐ Datos de localización

☐ Sobre condenas ☐ Otros:

_____

Infracciones penales.

Categorías especiales de datos ☐ Sobre el origen r ial ☐ Sobre la opinión política

☐ ☐ ☐

Sobre la religión o creencia Sobre la afiliación sindical Sobre la vida sexual

☐ ☐

☐ De salud ☐ Genéticos ☐ Biométricos

☐ ☐

Desconocidos Otros:

_____

Número aproximado de registros de datos personales afectados:

_____

8. Sobre los sujetos afectados

Perfil de los sujetos afectados:

☐ ☐ ☐ ☐

Clientes Usuarios Empleados

Suscriptores

☐ ☐

☐Estudiantes Pacientes Otros:

_____

Número aproximado de personas afectadas:

_____

9. Posibles consecuencias

Brecha de confidencialidad:

☐ ☐

Divulgación a terceros / difusión en internet Los datos pueden ser explotados ☐ con otros fines

Enriquecimiento de otras bases de datos Otras:

_____

Brecha de integridad:

☐ ☐

Datos han sido modificados, aunque hayan quedado inservibles o irrecuperables

Datos han sido modificados y utilizados para otros afines

☐

Otras:

_____

_____

Naturaleza del impacto potencial sobre los sujetos:

☐

Pérdida de control sobre sus

☐

Limitación de

sus derechos

☐

Discriminación

Datos personales

☐ ☐ ☐

Usurpación de identidad Fraude Pérdidas financieras

Reidentificación no autorizad

☐

Perdida de confidencialidad de datos afectados por secreto Profesional

☐

Daños a la reputación ☐ Otras:

_____

○ ○

Severidad de las consecuencias para los individuos: ○ Baja ○ Media

Alta Muy Alta

Medidas tomadas para solucionar la brecha y minimizar el impacto sobre los afectados:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

10. Comunicación a los interesados

¿Se ha comunicado la brecha a los interesados?

○

Si Fecha en la que se informó: _____

Número de sujetos informados: _____

Medios o herramientas de comunicación:

_____

○ No, pero serán informados Fecha en la que se informará: _____

○ No serán informados Justificación para no informar:

○ _____

Pendiente de decidir

_____

(Adjuntar contenido de la comunicación a los interesados)

11. Implicaciones transfronterizas

☐

¿Hay sujetos de otros Estados miembros de la UE afectados por la brecha?

☐

¿Hay sujetos de otros Estados fuera de la UE afectados por la brecha?

12. Documentos adjuntos
(adjuntar documentos)

En_____, a_____de_____2023

ANEXO 2: ANÁLISIS DE RIESGOS

Matriz de riesgos con Evaluación de Impacto relativa a la Protección de Datos (EIPD) Art. 42 LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES.

Maestrante: Alexandra Maldonado
Maestrante: Claudio Cortés

El Art. 42 de la LODPDP dispone: "Evaluación de impacto del tratamiento de datos personales.- El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera".

La Evaluación de Impacto en la Protección de Datos Personales (EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable.

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

Factores de riesgo que se derivan del fin declarado del tratamiento y otros fines vinculados al propósito principal.

OPERACIONES RELACIONADAS CON LOS FINES DE TRATAMIENTO				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Perfilado	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Aplicación de mejores prácticas de perfilado para prevenir conflictos con datos personales
Evaluación de sujetos	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Predicción	No aplica			
Control del empleado	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Contratos con clausulas especificas de compromiso para la proteccion de datos personales.
Acceso a internet	Aplica	Alta	Limitadamente mitigado	1. Politicas, procedimientos y manual de seguridad y privacidad de la información 2. Controles de acceso a internet
Observación comportamiento crediticio o preferencias en internet	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Monitorización	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Supervisión empleados y otros	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Contratos con clausulas especificas de compromiso para la proteccion de datos personales. 6. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Rastreo de contactos familiares y terceros	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Control físico de acceso	Aplica	Muy alta	Limitadamente mitigado	1. Politicas, procedimientos y manual de seguridad y privacidad de la información 2. Sistema de Control de Accesos. 3. Sistema de video vigilancia con IA, para identificar salida física de información.
Localización, geolocalización	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Aplicar mejores prácticas para metadata, donde se tenga previsión de gestión de la información de localización y geolocalización asociada a los archivos de la organización.
Identificación unívoca	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Ejecución de acciones técnicas de correlación y análisis para determinar relaciones de bases de datos que arrojan información de identificación unívoca.
Decisiones Automatizadas sin intervención humana	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Afinar los casos de uso de los motores de automatización para una adecuada gestión de los resultados de información que arrojan, así como un adecuado almacenamiento.
Tratamiento automatizado para soporte a toma de decisiones	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Afinar los casos de uso de los motores de automatización para una adecuada gestión de los resultados de información que arrojan, así como un adecuado almacenamiento.
Decidir sobre, o impedir, el ejercicio de derechos fundamentales	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Implementación de aplicativo para facultar al dueño de la información a gestionar sus datos.

Decidir sobre el control del interesado de sus datos personales	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Implementación de aplicativo para facultar al dueño de la información a gestionar sus datos.
Decidir sobre el acceso a un servicio	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Implementación de aplicativo para facultar al dueño de la información a gestionar sus datos.
Decidir sobre la realización o ejecución de un contrato	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Decidir sobre el accesos a servicios financieros	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular ; 4. Contratos de encargado de tratamiento de datos con cláusulas especiales.
Efectos jurídicos sobre las personas	Aplica	Media	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular ; 4. Contratos de encargado de tratamiento de datos con cláusulas especiales.
Evaluación y/o predicción de enfermedad/salud genéticamente	Aplica	Alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular ; 4. Contratos de encargado de tratamiento de datos con cláusulas especiales.
Conservación con fines de archivo	Aplica	Alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion;

Factores de riesgo relacionados con el ámbito del tratamiento que se derivan de los datos recogidos, procesados o inferidos en el tratamiento.

TIPOS DE DATOS UTILIZADOS				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Documentos personales	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion;
Información de aplicaciones de registro de actividades vitales o con fines médicos	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Aspectos personales	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Preferencias de consumo, gustos, hábitos (no categorias especiales)	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion; 5. Aplicar mejores prácticas para metadata, donde se tenga previsión de gestión de la información de localización y geolocalización asociada a los archivos de la organización.
Rendimiento laboral	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Situación económica	No aplica			
Estado financiero	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Contrato de encargado del tratamiento de datos con cláusulas especiales;
Medios de pago	No aplica			
Datos de comportamiento	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion

Datos de localización	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos sanitarios	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Datos biométricos	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Datos genéticos	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Categorías especiales de datos o que permitan inferirlos	No aplica			
Categorías especiales de datos seudonimizados	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Datos personales relativos a condenas e infracciones penales (o administrativas)	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Metadatos	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. Aplicar mejores prácticas para metadata, donde se tenga previsión de gestión de la información de localización y geolocalización asociada a los archivos de la
Identificadores únicos de identidad	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Datos y metadatos de la comunicaciones electrónicas	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Datos de navegación web	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Factores de riesgo relacionados con el ámbito del tratamiento relativos al número de sujetos afectados, la diversidad de datos o aspectos tratados, la duración en el tiempo, el volumen de datos, la extensión geográfica, la exhaustividad sobre la persona, la frecuencia de recogida, etc.

EXTENSIÓN Y ALCANCE DEL TRATAMIENTO				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Sistemático conforme un sistema organizado	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Exhaustivo y gran variedad de datos sobre las personas	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Involucra gran número de sujetos	No aplica			
El volumen de datos tratado es muy elevado	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Duración del tratamiento elevada	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Actividad del tratamiento de gran alcance geográfico	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Tratamiento a gran escala	No aplica			
Recopilación excesiva de datos con relación al fin del tratamiento	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

Factores de riesgo relacionados con el ámbito del tratamiento relativos a la categoría de interesados, como empleados, menores, mayores, personas en situación de vulnerabilidad, víctimas, discapacitados, etc.

CATEGORIAS DE INTERESADOS				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Menores de 14 años	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Víctimas de violencia de género	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Menores dependientes de sujetos vulnerables	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Persona bajo guardia y custodia d víctimas de violencia de género	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Mayores con discapacidad	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Personas mayores	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Personas con enfermedades mentales	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Discapacitados	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Personas que acceden a servicios sociales	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

Sujetos en riesgo de exclusión social	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Empleados	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Solicitantes de asilo	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Pacientes/Examenes ocupacionales	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Sujetos vulnerables	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Factores de riesgo que se derivan de la naturaleza del tratamiento al implementarse con determinadas características técnicas o tecnologías.

FACTORES TÉCNICOS DEL TRATAMIENTO				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Sistema de información hospitalaria	No aplica			
TV interactiva	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Servicios web	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Aplicaciones móviles	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Sistemas de registro de localización	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Reconocimiento facial	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Huella dactilar/datos biométricos	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
IoT (Internet de las Cosas)	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.

Uso innovador o nuevas soluciones organizativas	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Uso innovador de tecnologías consolidadas	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Tecnologías combinadas con otras	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Nuevas tecnologías	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Alto grado de fragmentación de los actores que intervienen en el desarrollo e implementación de los productos/servicios que implementan el	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Tratamientos automatizados	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Sistema inteligente	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Videovigilancia	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

Factores de riesgo que se derivan de la naturaleza del tratamiento al recogerse o generarse datos de forma específica.

RECOGIDA Y GENERACIÓN DE DATOS				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Acceso a bases de datos de referencia de crédito	No aplica			
Acceso a bases de datos sobre fraude	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Acceso a bases de datos sobre blanqueo de capitales o financiación del terrorismo	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Datos personales obtenidos en zonas de acceso público	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Recogida de datos de los medios sociales públicos	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Recogida de datos de redes de comunicaciones	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Recogida de datos de aplicaciones	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Datos procedentes de dos o mas tratamientos con finalidades diferentes	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Datos procedentes de dos o mas	No aplica			
Asociación de conjuntos de datos	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

Combinación de conjuntos de datos	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Enlaces de registros de base de datos de dos o mas tratamientos con finalidades o responsables diferentes	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Recogida de datos por un responsable distinto al que trata y aplica excepción de información	Aplica	Alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Falta de transparencia del momento preciso de la recogida de datos	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Nuevas formas de recogida de datos con riegos para derechos y libertades	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Factores de riesgo que se derivan del contexto del tratamiento al poder generarse consecuencias no contempladas en los propósitos originales previstos del tratamiento.
Se ha evaluado el nivel de riesgo con la probabilidad de que estas amenazas se materialicen en su tratamiento.

EFECTOS COLATERALES DEL TRATAMIENTO				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Excede las expectativas del interesado	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Posible reversión no autorizada de la seudonimización	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Posible pérdida de control por el responsable de los datos procesados por el encargado del tratamiento	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Riesgo de reidentificación de usuarios	No aplica			
Podría determinar la situación financiera	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Podría determinar la solvencia patrimonial	Aplica	Muy alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Podría deducir información relacionada con categorías especiales de datos	No aplica			
Pudiera privar a los afectados de sus derechos y libertades	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Pudiera impedir el control sobre sus datos personales	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

Puede provocar exclusión	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Puede provocar o genera discriminación	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Posible usurpación de identidad	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Posible fraude	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Posible daño reputacional	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Posible perjuicio económico significativo	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Posible perjuicio moral significativo	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;
Posible perjuicio social significativo	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales.
Posible pérdida de confidencialidad de datos sujetos al secreto profesional	Aplica	Baja	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion

Podría impedir el ejercicio de un derecho	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Podría impedir el acceso a un servicio	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Podría impedir el acceso a un contrato	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Podría recoger datos personales distintos de los usuarios de servicio	Aplica	Alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion
Posible manipulación de las personas	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Posibilidad de autocensura	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Posibilidad de provocar un cambio cultural para claudicar derechos y libertades	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Usos imprevistos o no deseados que pudieran afectar a derechos fundamentales	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

Factores de riesgo que se derivan del contexto específico del sector de actividad, modelo de negocio o tipo de entidad.
En este caso, entendido generalmente para tratamientos que no forman parte de los procesos de soporte de la entidad.

CATEGORÍA DEL RESPONSABLE / ENCARGADO				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Sociedad de la información	Aplica	Alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Empresa de biotecnología	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Mercadotecnia	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Hospitales	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales. 6. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Investigadores privados	Aplica	Baja	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Entidad de evaluación de información crediticia	No aplica			
Entidad de evaluación de fraude	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.

Entidad financiera	Aplica	Muy alta	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminación. 5. Contrato de encargado de tratamiento de datos con cláusulas especiales. 6. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Empleador	Aplica	Alta	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Proyectos de investigación	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.
Ensayos clínicos	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos. 5. En medida de lo posible, exigir a los terceros reciprocidad en el tratamiento de datos personales.

Factores de riesgo que se derivan del contexto en el que se realizan las comunicaciones de datos a terceros en el marco del tratamiento.

COMUNICACIONES DE DATOS				
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Mitigación**	**Control aplicado**
Transferencia habitual a estados u organizaciones en otros países sin un adecuado nivel de protección	Aplica	Muy alta	No mitigado	1. Contratos de encargado de tratamiento de datos con empresa filial en el extranjero, incluyendo cláusulas especiales. 2. Posible Tranferencia internacional de datos con requerimiento de autorización de la autoridad cuando sea
Falta de transparencia de los actores involucrados en el tratamiento	Aplica	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

OTROS FACTORES DE RIESGO ESPECÍFICOS DEL TRATAMIENTO					
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Impacto**	**Mitigación**	**Control aplicado**
Pérdida de información en archivos físicos o digitales	Aplica	Baja	Limitado	Limitadamente mitigado	1. Politicas, procedimientos y manual de seguridad y privacidad de la información 2.Procedimiento de gestion documental de archivo y eliminacion
Prolongado almacenamiento de archivos físicos o digitales	Aplica	Baja	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.

SEGURIDAD EN LOS TRATAMIENTOS					
Tipo de riesgo	**Aplicabilidad**	**Probabilidad**	**Impacto**	**Mitigación**	**Control aplicado**
Pérdida de confidencialidad	Aplica	Alta	Limitado	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Pérdida de integridad	Aplica	Baja	Limitado	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Pérdida de disponibilidad	Aplica	Baja	Limitado	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion.
Pérdida de trazabilidad	Aplica	Baja	Muy limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion.
Pérdida de autenticidad	Aplica	Baja	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Deficiencias en resiliencia	Aplica	Baja	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4. Actas de reuniones de comités en los que se incorpora la gestión del tratamiento de datos.
Fallos en medidas y garantías técnicas de protección de datos	Aplica	Baja	Limitado	Significativamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular; 4.Procedimiento de gestion documental de archivo y eliminacion. 5.Clausulas para contratistas con el cumplimiento del tratamiento de datos
Errores en las operaciones técnicas de tratamiento	Aplica	Baja	Media	Limitadamente mitigado	1. Convenios de confidencialidad. 2. Politicas, procedimientos y manual de seguridad y privacidad de la información 3. Aceptacion de tratamiento de datos del titular;

ANEXO 3: EVALUACIÓN DE IMPACTO

	MATRIZ DE EVALUACIÓN DEL IMPACTO DEL NEGOCIO (BIA)				
	Fecha de emisión			Código de documento	Nivel de confidencialidad
	1/2/23			RAD-REG	RESTRINGIDO

01. Identificación de los productos y servicios críticos – BIA estratégico

Producto/ Servicio	Descripción del Producto/ Servicio	Impacto			Puntaje	Nivel de impacto
		Financiero	Reputación	Legal y regulatorio		
Diversidad de equipos integrados	Equipos Tecnológicos de diferentes fabricantes que se encuentran integrados para dar un servicio específico.	4	5	2	11	No critico
Recolección, retención de logs	Todo equipo tecnológico genera archivos en los que se guarda las acciones o eventos que suceden dentro de los mismos, estos archivos se alamcenan o recolectan en un repositorio para su análisis.	4	5	3	12	No critico
Análisis de logs y monitoreo de eventos de seguridad	Equipo Tecnológico especializado en analizar los archivos generados de los eventos de seguridad de una infraestructura tecnológica.	4	5	4	13	No critico
Identificación de amenazas de seguridad	Tanto el software como el hardaware tienen defectos de fabricación, dichos defectos probocan vulnerabilidades que se convierten en amenaza de seguridad ya que pueden ser explotadas causando daños a la infraestructura y robo de información.	5	5	5	15	No critico
Gestión de incidentes y reportes	Un incidente es un resultado de falla o error en la infraestructura tecnológica, los reportes son generados para notificar el estado de los insidentes reportados o soluciones que se han generado a los incidentes.	4	4	2	10	No critico
Reacción ante amenazas	Una vez que se ha detectado amenzas de seguridad, se tiene que dar un tratamiento o solución y que no cauce daños o pérdida de información.	4	5	4	13	No critico
Control ante amenazas	Realizar un adecuado control del estado de las amenzas para su tratamiento y posible solución.	4	5	4	13	No critico
Soluciones con medidas preventivas	Realizar mantenimiento preventivos para aplicar parches de seguridad que corrigen vulnerabilidades en el software o Hardware, utilizar las mejores prácticas de gestión de la tecnología.	4	5	5	14	No critico
Servicio de Infraestructura	Proveer servicios de venta de equipos informáticos con su respectiva implementación, configuración, garantía, mantenimiento y soporte	3	4	3	10	No critico
Servicio de Ciberseguridad						
Servicio de SOC/CSIRT						

Nota 1: Se considera como críticos aquellos productos/ servicios que superan un puntaje de 15.
Nota 2: El SGCN se aplicará para los productos de mayor utilidad que ingresen dentro del Pareto 80%

2. Identificación de procesos críticos – BIA táctico

Procesos de la organización	Productos/ servicios escogidos para la aplicación del SGCN									
	Diversidad de equipos integrados	Recolección, retención de logs	Análisis de logs y monitoreo de eventos de seguridad		Gestión de incidentes y reportes	Control ante amenazas	Soluciones con medidas preventivas	Servicios de Infraestructura	Servicios de Ciberseguridad	Servicios de SOC /CSCIRT
Gestión de la Dirección								X		
Planeación y Gestión Financiera								x		
Sistema Integrado de Gestión								x		
Estrategia, Monitorizacion y Control de Ventas								x		
Gestión de Acuerdos con Proveedores								x		
Comercial								x		
Gestión Integrada de Proyectos										
Ciberseguridad										
Infraestructura	X	X	X		X	X	X	x		
SOC CSIRT - SOC								x		
Servicio Posventa								x		
Gestión de Seguridad de la Información								x		
Gestión de TI interno & Service Desk	X	X	X		X	X	X	x		
Gestión de compras	X	X	X		X	X	X	x		
Gestión de la continuidad	X	X	X		X	X	X	x		
Gestión de Talento Humano	X	X	X		X	X	X	x		
Marketing e Imagen Corporativa										

2.2 Criticidad según proceso asociados a los productos/ servicios

Proceso	Descripción del proceso	Impacto			Nivel de impacto
		Financiero	Contractual	Objetivos del negocio	
Gestión de la Dirección	Revisión del Sistema de Gestión de Calidad por parte de la Gerencia General, en relación con la conveniencia, adecuación y eficacia continua de los procedimientos de la empresa.	3	2	5	No Crítico
Planeación y Gestión Financiera	Planeación financiera es el proceso mediante el que se decide cómo se utilizarán los recursos de la empresa para alcanzar los objetivos planteados con anterioridad.	2	2	3	No Crítico
Sistema Integrado de Gestión	Implementar y mantener el sistema integrado de gestión	1	1	1	No Crítico
Estrategia, Monitorizacion y Control de Ventas	Alinear las acciones de los vendedores con los objetivos organizacionales, monitoreando el desempeño del equipo, la cantidad de oportunidades abiertas y de cierre.	2	3	5	Crítico
Gestión de Acuerdos con Proveedores	Relaciones con proveedores de bienes y servicios para las operaciones diarias.	3	1	3	No Crítico
Comercial	Facilitar la interacción entre empresa y clientes, estableciendo qué servicios se deben ofertar y cuáles no.	3	2	4	No Crítico
Gestión Integrada de Proyectos	Asegurar la ejecución óptima de los proyectos	5	4	3	Crítico
Infraestructura	Optimización de recursos y un correcto funcionamiento de aplicaciones y sistemas, para brindar una atención efectiva para los procesos de negocio y requerimientos de mercado.	5	5	5	Crítico
Ciberseguridad	Operaciones de seguridad detectando actividades maliciosas antes de que puedan causar un daño.	2	3	5	No Crítico
SOC CSIRT - SOC	Operaciones de seguridad detectando actividades maliciosas antes de que puedan causar un daño.	2	3	5	No Crítico
Servicio Posventa	Procesos que se realizan después de haber completado una venta asegurando una buena experiencia al comprador y, de esta forma, asegurar su fidelidad.	2	3	5	No Crítico
Gestión de Seguridad de la Información	Establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la	2	3	5	No Crítico

	información				
Gestión de TI Interno & Service Desk	Garantizar la operatividad de los equipos informáticos y proporcionar el servicio de Service Desk	4	4	4	Crítico
Gestión de compras	Adquirir bienes y servicios que la empresa necesita, garantizando el abastecimiento de las cantidades requeridas en términos de tiempo, calidad y precio.	2	4	5	Crítico
Gestión de la continuidad	Planes de continuidad a través de actividades y procedimientos que permitan hacer frente a un evento disruptivo, con el objetivo de reanudar y posteriormente restaurar las operaciones.	5	5	5	Crítico
Gestión de Talento Humano	Identificación de competencias profesionales, actitudes y aptitudes que necesita reunir el personal para desempeñar correctamente sus funciones.	3	4	3	No Crítico
Marketing e Imagen Corporativa	Percepción del público sobre la empresa, el conjunto de creencias, actitudes, ideas, prejuicios y sentimientos de los consumidores sobre la empresa.	2	2	4	No Crítico

Nota 1: Se considera como críticos aquellos procesos que superan un puntaje de 15.

3. Identificación de actividades asociadas a procesos críticos - BIA operativo

Proceso crítico	Actividades
Gestión de la Dirección	Representar judicial y legalmente a la empresa
	Elaborar la planificación estratégica
	Seguimiento de la planificación estratégica
	[illegible]
	Seguimiento al cumplimiento del presupuesto anual y gestionar los recursos para el SGI
	Aprobación de la documentación de la empresa
Planeación y Gestión Financiera	Presupuesto y Contabilidad
	Controles Financieros y no Financieros
Sistema Integrado de Gestión	Implementación de los sistemas de gestión
	Mantenimiento de los sistemas de gestión
	Comunicaciones de Partes Interesadas.
	Gestión de los informes de auditoria.
	Gestión de la matriz de cumplimiento legal.
	Gestión del formato de solicitud de acción
	Leyes, reglamentos nuevos o modificados.
Estrategia, Monitorizacion y Control de Ventas	Oportunidad registrado en el CRM
	Requerimientos de oportunidades
	Atención a necesidad de TI
Gestión de Acuerdos con Proveedores	[illegible] fabricante
	E-mail de confirmación, verificando el usuario y contraseña asignado
	Requerimiento de productos o servicios de fabricantes
	Correo de caducidad de oportunidades
	Confirmación de suspensión o extensión de oportunidad
	Acuerdos y compromisos de seguimientos al CRM
Comercial	[illegible] mayor y mejor posición en el mercado.
	Representar a la Empresa en aspectos comerciales ante fabricante, mayoristas, negociar convenios y administrar los contratos que se suscriban con éstos.
	[illegible] servicios que ofrece la Empresa.
	[illegible] negocio.
	Identificar procesos en portal público
	Presentar ofertas en portales o clientes
	Participar en subastas
	Controlar que los objetivos, planes y programas se cumplan en los plazos y condiciones establecidos.
	Establecer ventajas competitivas donde se ofrezcan servicios de la Empresa, procurando obtener las mejores participaciones en el mercado.
	[illegible] de la empresa.
Gestión Integrada de Proyectos	Notificación de suscripción de contrato u orden de servicio.
	Designación del Proyecto
	Planificación del Proyecto
	[illegible]
	Cierre del Proyecto
Ciberseguridad	Apoyar a la gestión de incidentes de seguridad informática
	Apoyar en la prestación de servicios proactivos, reactivos, manejo de instancias y en la gestión de calidad de la seguridad.
	[illegible]
	Participar en eventos de la comunidad del CSIRT
	Realizar el respectivo escalamiento y seguimiento de la solución de incidentes que no puedan ser atendidos en el CSIRT
	Realizar [illegible]
	Brindar soporte a soluciones
	[illegible]
SOC CSIRT - SOC	Validación del cumplimiento de SLA's
	Coordinación 24x7 de actividades Ingenieros N2
	Coordinación 24x7 de actividades Ingenieros N1
	Análisis permanente de nuevas ciber amenazas
	Recepción de requerimientos por parte del cliente
	Atención de incidentes 24x7
	Investigación de nuevas tecnologías y métodos para detección de ataques
	[illegible] presentaciones
	Administrar eficientemente los recursos de la empresa.
	Validación del cumplimiento de SLA's. (si)
	Coordinación de actividades del Analista CSM.

Proceso crítico	Actividades	Proceso soporte de las actividades
Gestión de Seguridad de la Información	Verificación que se haya aperturado un tickets de Incidencia/problema con prioridad alta en plataforma PROACTIVANET; y que estos hayan sido escaados a las pernas correspondientes.	Gestión de Seguridad de la Información
	Recibe respuesta de las acciones tomadas por parte del Área de Operaciones (Incluido el equipo de CSIRT), referente al tratamiento del incidente informado. -Si las acciones fueron efectivas se incluye dicha información diligenciando a través de plataforma PROACTIVANET - Atención de incidente de seguridad informática para cerrar el incidente.	
	Reporta al Gerente General el incidente de seguridad informática ocurrido y las acciones tomadas para mitigar y/o corregir sus implicaciones.	
	[illegible] caciones disciplinarias y/o penales.	
	Archiva los documentos e información asociada al incidente de seguridad informática.	
Infraestructura	Monitoreo de la infraestructura tecnológica	Infraestructura
	Obtención de respaldos de información	
	Mantenimientos preventivos de infraestructura tecnológica	
	Despliegue e implementación de equipos tecnológicos	
	Soporte técnico de segundo nivel	
	Servicio del SOC - gruporadical.net	
	Gestión de niveles de servicio	
Gestión de TI Interno & Service Desk	Gestión de incidentes	Gestión de TI Interno & Service Desk
	Atención de tickets de soporte técnico	
	Configuración de servicios internos de Tecnología	
	[illegible]	
	Gestión de la capacidad	
Gestión de la continuidad	Análisis de riesgos	Gestión de la continuidad
	Análisis de impacto al negocio	
	Recuperación ante desastres	
	Gestión de crisis	
	Pruebas del plan de continuidad	
Gestión de compras	Compras	Gestion de compras
	Controla el número de orden de compra	
	Recibe requerimiento de compra del área administrativa	
	Solicita cotizaciones	
	Recibe órdenes de compra tecnicas	
	Envía órdenes de compra técnica y adminstivas al proveedor batrave de mails	
	En algunos casos acuerda la firma de pago	
	Gestiona la entrega recepción del producto	
	Entrega [illegible]	
Gestión de Talento Humano	Recibir la requisición de personal.	Gestion de Talento Humano
	[illegible] (pre-selección)	
	Entrevistar a los/las candidatos pre-seleccionados.	
	Aplicar las pruebas de conocimientos	
	[illegible]	
	Coordinar los exámenes pre-ocupacionales.	
	Entrevistar al candidato	
	Elaborar el contrato de trabajo e ingreso al IESS.	
	Realizar la inducción administrativa.	
	Elaborar el plan de recompensas e incentivos laborales	
	Elaborar los planes y programas de capacitación anual	
	[illegible]	
	Verificar la eficacia de la capacitación.	
Marketing e imagen corporativa	Selección de contenido de tendencias de ciberseguridad para redes sociales.	Marketing e imagen corporativa
	Coordinación y desarrollo de presentaciones y comunicaciones	

	MATRIZ DE ANALISIS DEL IMPACTO DEL NEGOCIO (BIA)				
	Fecha de emisión			Código de documento	Nivel de confidencialidad
	1/2/23			RAD-REG	RESTRINGIDO

Servicio Posventa	Atención de incidentes, problemas y requerimientos.
	Reportes de Trabajo
	Control de actividades del Personal relacionadas con la atención y gestión de incidentes y requerimientos.
	Revisión de informes y reportes. (si)
	Soporte en COMPLIANCE por exámenes de auditoría. (n/a)
	Cumplir con las disposiciones establecidas en el Código de Conducta Anticorrupción, Manual del Sistema Integrado de Gestión, Reglamento Interno de Trabajo, Reglamento de Higiene y Seguridad, Procedimientos y Políticas de las normas que forman parte del Sistema Integrado de Gestión.
	Reportar eventos de soborno, privacidad de la información o que atente con la protección de datos personales u otra que afecte los procesos y continuidad del negocio.
	Cumplir con la normativa técnico legal de los clientes, partes interesadas, normas y estándares que aplica a la empresa.
	Evaluación de infraestructura para servicio
	Apoyar en dar asistencia en temas de la parte legal que la empresa lo requiera.
	Asistir y recomendar mejoras que se estimen necesarios en las soluciones que se ofertan.
	Recomendar posibles productos y servicios para ser comercializados.

4. Determinación de RTO, RPO, MTPD

RPO (Recovery Point Objetive): El punto objetivo de recuperación. Hace referencia a la cantidad de información que la empresa está dispuesta a perder ante algún incidente que amenace la continuidad de sus operaciones. Para determinar el valor de este parámetro, con los dueños de los procesos, se identificó el lugar de almacenamiento de la información que se gestiona en cada proceso, a efectos de determinar la frecuencia con la que se realiza el backup a las bases de datos y servidores que almacenan dicha información.
¿Qué es RPO? El objetivo de punto de recuperación (RPO) generalmente se refiere a la cantidad de datos que se pueden perder dentro del período más relevante para una empresa, antes de que ocurra un daño significativo, desde el punto de un evento crítico hasta la copia de seguridad con mayor precedencia

RTO (Recovery Time Objetive): El tiempo objetivo de recuperación. Es el tiempo que tiene una organización para poder reanudar sus operaciones y continuar brindando el producto o servicio afectado. El RTO se calcula simulando la ejecución de un proceso considerando la ausencia de principales factores tales como, personal clave, sistemas sobre los cuales se soporta las operaciones, proveedores importantes y similares.
¿Qué es RTO? El objetivo de tiempo de recuperación (RTO) a menudo se refiere a la cantidad de tiempo que una aplicación, sistema y/o proceso puede estar inactivo sin causar un daño significativo a la empresa, así como el tiempo dedicado a restaurar la aplicación y sus datos.

MTPD (Máximum Tolerable Period of Disruption): El período máximo de interrupción tolerable está referido al tiempo máximo que tiene la organización para tener inoperativo sus negocios, antes de que dicha inoperatividad comience a generar pérdidas graves para la empresa, y pongan en riesgo la continuidad de la misma. Para poder establecer el MTPD, se debe tener en cuenta el apetito al riesgo definido por la empresa. Para establecer dicho apetito, la organización ha considerado los cinco tipos de impacto cuantificables: Financiero, Imagen y Reputación, Legal o regulatorio, Contractual, Objetivos del negocio.
Tiempo máximo tolerable de interrupción (MTPD): límite máximo de indisponibilidad, que se establece para señalar el momento en que se considera continuar con la actividad o restauración de productos y/o servicios

Tipo de impacto	Tiempos de inoperabilidad										
	1 hr	4 hr	8 hr	12 hr	24 hr	2 día	3 días	<2 semana	RPO		MTPD
Financiero	--	--	--	--	--	--	--	--	__horas		__horas
Imagen y Reputación	--	--	--	--	--	--	--	--	__horas		__horas
Legal o regulatorio	--	--	--	--	--	--	--	--	__horas		__horas
Contratual	--	--	--	--	--	--	--	--	__horas		__horas
Objetivos del negocio	--	--	--	--	--	--	--	--	__horas		__horas

Producto/ Servicio	Proceso	Actividad	Registros vitales	Equipos/ Recursos	Sistemas de información/ Aplicaciones	Servicios	RPO (horas)	DESCRIPCIÓN RPO	RTO (horas)	DESCRIPCIÓN RTO	MTPD (horas)	RIESGO	RESUMEN MTPD	REF MTPD	Evaluación (Seguimiento y controles de Riesgos y Oportunidades) (Revisión Semestral)		
															Seguimiento de las acciones preventivas y control	Fecha de verificación	Estatus
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Gestión de la Dirección	Representar judicial y legalmente a la empresa.	Acta de la junta de socios, Registro mercantil, Registro de la Superintendencia de compañías, RUC actualizado con el representante legal, Registros bancarios, Registro de MT, Registro IESS.	Computador portatil, impresora, equipo celular	Aplicaciones bancarias, páginas web Supercias, SRI, MT, IESS.	Energía eléctrica Internet, Datos, telefonía movil	72	Tiempo máximo para mantener sin representar judicial y legalmente a la empresa.	40	Tiempo estimado de recuperación para atener la representar judicial y legal de la empresa.	80	No contar con la representación legal y judicial para la firma de documentos legales. Causaría insertidumbre en las partes interesadas	Financiero:3 días; - Imagen y Reputación :24 horas; - Legal o regulatorio:2 días; - Contractual:3 días; - Objetivos del negocio:3 días	ACT 1	Plan de continuidad del negocio	19/12/22	Gestionado
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Planeación Financiera	Presupuesto y Contabilidad	Estados financieros, comprobantes de ingresos egreso, retenciones, facturas. Contabilidad en el sistema contable. Gestión de cartera de clientes y gestión de proveedores.	Computador portatil auxiliar contable / computador Contador General / Computador Directors Administrativa Financiera - Servidor al que estan conectados / internet	FINETIME	Sistema Contable Plataforma de cash management de las entidades financieras	Depende del acceso al servidor y la habilitación del VPN	Documentos y datos ingresados en el sistema contable: facturas de compra, venta, retenciones, diarios, egresos, ingresos, procesos de pagos y cobros.	3 horas	La contabilidad y la información financiera es un registro de las operaciones realizadas por lo cual puede demorar hasta un dia, ya que depende del requerimiento	Tiempo estimado es de 24 horas que se ingresa al sistema de acuerdo con la necesidad y no poder emitir documentos para atención a clientes y realizar pagos urgentes a proveedores críticos	- Riesgo de pérdida de información que se encuentra en el servidor. - Riesgo de demora en pago y cobros por imposibilidad de ingreso a las plataformas de las intituciones financieras	Financiero:2 horas; - Imagen y Reputación :4 horas; - Legal o regulatorio:0,5 horas; - Contractual:0,5 horas; - Objetivos del negocio:0,25 horas	ACT 2	Plan de recuperación ante desastres tecnológicos	31/3/23	Programado simulacro 03/2023
		Controles Financieros y no Financieros	Arqueos,,conciliaciones bancarias, segregación de funciones, Firmas de contratos, cumplimiento de obligaciones	Computador portatil auxiliar contable / Computador Contador General / Computador Gerente Administrativo Financiero / Computador Directora Administrativo Financiero - Servidor al que estan conectados / internet	FINETIME Excel Firma EC IESS SRI SUPERCIAS SERCOP Municipio	Sistema Contable Microsoft office Firma EC	Depende del acceso al servidor y el acceso a conectividad de internet	Documentos físicos como: ordenes de compra autorizados, correos, transferencia bancarias, contratos, declaraciones.	3 horas	3 horas en reestablecer los controles financieros y no financieros	24 horas en reactivación de controles para cunmplimiento	* Riesgo de incumplimiento de obligaciones tributarias, laborales y societarias * Riesgo de imposibilidad de supcripcion de contratos nuevos	Financiero:1 hora; - Imagen y Reputación :1 hora; - Legal o regulatorio:4 horas; - Contractual:1 hora; - Objetivos del negocio:1 hora	ACT 3	Plan de recuperación ante desastres tecnológicos	31/3/23	Programado simulacro 03/2023
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Sistema Integrado de Gestión	Implentación de sistemas de gestión	Programa anual de actividades	Estación de trabajo. Computador. Teléfono. Presupuesto para asesores	Información compartido. Office 365 - Shared Point	Energía eléctrica. Servicio de telefonía. Servicio de internet.	40 horas	Retardo en las actividades de implementación y no afecta a la planificación	80 horas	Tiempo en el cual empesaría afectar la planificación de la implementación	120 horas	Demoras de acuerdo a la planificación de implementación de los sistemas de gestión.	Financiero:4 horas; - Imagen y Reputación :2 horas; - Legal o regulatorio:1 horas; - Contractual:12 horas; - Objetivos del negocio:24 horas	ACT 4	Programa actividades	19/12/22	Gestionado
		Mantenimiento de los sistemas de gestión	Programa anual de actividades	Estación de trabajo. Computador. Teléfono. Presupuesto para el asistente.	Información compartido. Office 365 - Shared Point	Energía eléctrica. Servicio de telefonía. Servicio de internet.	16 horas	Retardo en las actividades de mantenimiento del SIG y no afecta a la planificación	32 horas	Tiempo en el cual empesaría afectar la planificación del mantenimiento del SIG	40 horas	Demoras de acuerdo a la planificación de mangtenimiento de los sistemas de gestión.	Financiero:N/A; - Imagen y Reputación : 6 horas; - Legal o regulatorio:N/A; - Contractual:6 horas; - Objetivos del negocio:1 horas	ACT 5	Programa actividades	19/12/22	Gestionado

	MATRIZ DE ANALISIS DEL IMPACTO DEL NEGOCIO (BIA)			
	Fecha de emisión		Código de documento	Nivel de confidencialidad
	1/2/23		RAD-REG	RESTRINGIDO

" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Estrategia, Monitorizacion y Control de Ventas	Registro de oportunidades en la plataforma CRM	Registro CRM	Computador	CRM	Internet Energia Electrica	10 minutos	En el tiempo de 10 minutos se realiza el registro de oportunidades	24 horas	Se puede dejar de ralizar esta actividad sin causar un daño significativo a la empres en un tiempo de 24 horas	5 días	No contar con información actualizada sobre las oportunidades cuando haya ausencia del personal a cargo	Financiero:N/A; - Imagen y Reputación :4 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:N/A	ACT 6	Plan de continuidad del negocio. Registro de oportunidades en la plataforma CRM	19/12/22	Gestionado
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Gestión de acuerdo con proveedores	Registro de oportunidades en los portales de los proveedores	Registro en portales de partner	Computador	Portal de Partners	Internet Energía Electrica	10 minutos	En el tiempo de 10 minutos se realiza el registro de oportunidades en los portales de partners	1 hora	Se puede dejar de ralizar esta actividad sin causar un daño significativo a la empres en un tiempo de 1 hora	24 horas	Perder beneficios comerciales al no registrar a tiempo la oportunidad	Financiero:N/A; - Imagen y Reputación :4 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:2 horas	ACT 7	Plan de continuidad del negocio. Registro de oportunidades en los portales de los proveedores	19/12/22	Gestionado
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Comercial	Identificar procesos en portal público	Términos y condiciones	PC, teléfono	Porta de compras pública	Energía eléctrica Teléfonía Celular Internet	8 horas	No se haya detectado a tiempo una oferta en el portal de la Sercop	16 horas	Se encuentra a tiempo para presentar la oferta sin participación inicial en el proceso (Ejemplo no se pudo realizar preguntas)	24 horas	No alcanzar a presentar ofertas en el portal	Financiero:4 horas; - Imagen y Reputación :1 horas; - Legal o regulatorio:5 hora; - Contractual:8 hora; - Objetivos del negocio:24 horas	ACT 8	Plan de continuidad del negocio.	19/12/22	Gestionado
		Presentar ofertas en portales o clientes	Oferta técnica. Oferta económica Catalogos, manuales	PC, teléfono	Porta de compras pública	Energía eléctrica Teléfonía Celular Internet	8 horas	No se haya preparado a tiempo una oferta para subir al portal	16 horas	Tiempo por finalizar para subir una oferta al portal	24 horas	No alcanzar a presentar ofertas en el portal	Financiero:2 horas; - Imagen y Reputación :1 hora; - Legal o regulatorio:8 horas; - Contractual:1 hora; - Objetivos del negocio:24 horas	ACT 9	Plan de continuidad del negocio.	19/12/22	Gestionado
		Participar en subastas	Oferta económicas en subasta	PC, teléfono	Sistemas de comunicación remitidos para subasta	Energía eléctrica Teléfonía Celular Internet	1 minuto	Tiempo en que se deconectó dentro de la subasta	2 minutos	Tiempo en que se puede perder la oportunidad por no estar en la subasta	3 minutos	No se pudo participar en la propuesta.	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 10	Plan de continuidad del negocio.	19/12/22	Gestionado
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Gestión Integrada de Proyectos	Notificación de suscripción de contrato u orden de servicio.	Contrato u Orden de Servicio. Oferta. Pliegos (en entidad pública). TDR. Acta de Negociación (cuando exista). Acta de preguntas y repuestas (Cuando exista). BOM.	Computador	Correo Electrónico Sharepoint Office 365	Energía eléctrica Teléfonía Celular	1 hora	Tiempo en llegar a otro sitio con acceso a internet	6 horas	6 horas para reestablecer la notificación de suscripción de contrato u orden de servicio.	24 horas	No se puede iniciar el proceso de planificación del proyecto No se puede realizar la reunión de kickoff del proyecto	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 11	Plan de continuidad del negocio.	19/12/22	Gestionado
		Designación del proyecto	Check list de entrega de documentación del área comercial a oficina de proyectos	Computador	Correo electrónico, llamada telefónica Sharepoint Office 365	Energía eléctrica	1 hora	Tiempo en llegar a otro sitio con acceso a internet	4 horas	Tiempo para entregar y notificar al PM designado el nuevo proyecto.	8 horas	No iniciar en las fechas estipuladas contractualmente	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 12	Plan de continuidad del negocio. Check list de entrega de documentación del área comercial a oficina de proyectos	19/12/22	Gestionado
		Planificación del proyecto	Reunión interna del proyecto, KickOff del proyecto	Computador Telefono movil	Correo electrónico, llamada telefónica	Energía eléctrica	1 hora	Tiempo en restablecer los servicios y software de proyecto	1 hora	Tiempo para agendar o re agendar reunión de planificación con el equipo ya sea presencial o virtual.	8 horas	No cumplir con las fechas de la planificación del proyecto	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 13	Plan de continuidad del negocio. Reunión interna del proyecto, KickOff del proyecto	19/12/22	En proceso
		Ejecución y Control del Proyecto	Project, Actas de reunión, Informes, Reportes, Matriz de Riesgos	Computador	Project, Sharepoint	Energía eléctrica	1 hora	Tiempo en restablecer los servicios y software de proyectos	1 hora	Tiempo para agendar o re agendar reunión de planificación con el equipo ya sea presencial o virtual.	24 horas	No cumplir con las fechas de la ejecución del proyecto	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 14	Project, Actas de reunión, Informes, Reportes, Matriz de Riesgos	19/12/22	En proceso
		Cierre del Proyecto	Project, Actas entrega recepción, Matriz de Riesgos, Lecciones Aprendidas	Computador	Project, Sharepoint	Energía eléctrica	1 hora	Tiempo en restablecer los servicios y software de proyectos	2 horas	Tiempo para entregar a el cliente documentos de cierre de proyecto y firmas respectivas.	48 horas	No cumplir con las fechas de la ejecución del proyecto	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 15	Project, Actas entrega recepción, Matriz de Riesgos, Lecciones Aprendidas	19/12/22	En proceso
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Ciberseguridad	Implementación de solución o proyecto	Ingeniería de detalle; Memoria técnica; Pruebas de aceptación (ATP)	Laptops de Ingenieros; Equipamiento involucrado en la solución.	Visio Microsoft Outlook office365."	Servicio electrico; Servicio de Internet; Servicio Offices 365; Servicio Microsoft Visio.	Tiempo maximo establecido de la implementación del proyecto	Cambio de recurso por implementacion en sitio y remoto	30 dias	Cambio de recurso en sitio y remoto sin multas.	29 dias	Cambio de recurso con pedido de prórroga y multa	Financiero:2 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:8 horas; - Contractual:24 horas; - Objetivos del negocio:1 mes	ACT 16	Plan de continuidad del negocio.	19/12/22	Gestionado
		Soporte de equipamiento	Informe técnico / SLA	Laptops de Ingenieros; Equipamiento involucrado en la solución.	ProactivaNET. Outlook office365. Aplicación Zoom; Teams	Servicio electrico; Servicio de Internet; Servicio Offices 365; Servicio	24 horas / 4 horas	Cambio de recurso por soporte en sitio o remoto.	4:30 horas	Cambio de recurso remoto sin multas, en sitio depende la ubicación, etc.	4 horas	Cambio de recurso con multa por cada hora de reetraso.	Financiero:1 mes; - Imagen y Reputación :2 días; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 17	Plan de continuidad del negocio Informe técnico / SLA	19/12/22	Gestionado

	MATRIZ DE ANALISIS DEL IMPACTO DEL NEGOCIO (BIA)			
	Fecha de emisión		Código de documento	Nivel de confidencialidad
	1/2/23		RAD-REG	RESTRINGIDO

		Mantenimientos preventivos de equipamiento	Informe técnico	Laptops de Ingenieros; Equipamiento involucrado en la solución.	ProactivaNET. Outlook office365. Aplicación Zoom; Teams	Servicio electrico; Servicio de Internet; Servicio Offices 365; Servicio	72 horas	Cambio de recurso por soporte en sitio.	48 horas	Cambio de recurso en sitio sin multas, depende de la ubicación	72 horas	Cambio de recurso con multa por cada hora de reetraso.	Financiero:8 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 18	Plan de continuidad del negocio. Informe técnico	19/12/22	En proceso
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	SOC CSIRT	Monitoreo SOC 24/7	Tickets de la mesa de ayuda ProactivaNET. Reportes diarios de casos gestionados.	Laptop. Maquinas virtuales. Telefono celular con linea y plan de datos activo	SIEM Qradar. SIEM Arcsigth. SIEM RSA. Darktrace. DDI. Nozomi. CASB. WHD. ProactivaNET. Outlook office365.	Conexión electrica. Conexión a internet. Acceso VPN Radical.	0,25	0,25 Minutos Monitoreo SOC 24/7	0,4		0,5	Incumpliento del SLA y del servicio contratado por los clientes	Financiero:2 horas; - Imagen y Reputación :8 horas; - Legal o regulatorio:24 horas; - Contractual:24 horas; - Objetivos del negocio:1 mes	ACT 19	Plan de continuidad del negocio. Tickets de la mesa de ayuda ProactivaNET. Reportes diarios de casos gestionados.	19/12/22	En proceso
" -Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas."	Servicio Posventa	Validación del cumplimiento de SLA's. (si)	Reporte mensual de SLA	Acceso directo al sistema Proactivanet desde una computadora	Proactivanet	N/A	10 minutos	Es una actividad que permite contar con los indicadores mensuales, más no afecta el servicio del cliente interno y externo.	10 minutos	Sino se realiza en este período de tiempo, no se tiene visibilidad para toma de decisiones estratégicas del siguiente período.	30 días (al finalizar cada mes)	Se puede obviar problemas que afectan los SLA	Financiero:2 horas; - Imagen y Reputación :4 horas; - Legal o regulatorio:1 hora; - Contractual:8 horas; - Objetivos del negocio:1 mes	ACT 20	Reporte mensual de SLA	19/12/22	En proceso
		Recepción de requerimientos por parte del cliente.	Llamadas telefónicas que son registradas en Tickets de requerimientos REQ	Teléfono movil	Proactivanet para registro del ticket	N/A	10 minutos	Esta actividad permite realizar una interacción directa con el cliente. Sin embargo los procedimientos exigen que se realice la llamada o envio del correo a la mesa de ayuda soporte@gruporadical.com	10 minutos	Sino se realiza en este período de tiempo, no existe afectación ya que el cliente debe optar por el método de notificación establecido en el procedimiento	10 días ya que el cliente	Se puede obviar problemas que afectan los SLA	Financiero:4 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:2 horas; - Contractual:12 horas; - Objetivos del negocio:24 hiras	ACT 21	Llamadas telefónicas que son registradas en Tickets de requerimientos REQ	19/12/22	En proceso
		Atención de incidentes, problemas y requerimientos.	tickets REQ, INC	Sistema de gestión de tickets, teléfono, computadoras	Proactivanet para registro del ticket	N/A	SLA de respuesta (10 minutos)	Esta actividad es para atender el servicio de soporte y mantenimiento	10 minutos	Sino se realiza esta actividad, afecta directamente al SLA de notificación del ticket asignado	10 minutos	Ejecución de multas por incumplimiento SLA	Financiero:24 horas; - Imagen y Reputación :12 horas; - Legal o regulatorio:12 horas; - Contractual:12 horas; - Objetivos del negocio:1 mes	ACT 22	Plan de continuidad del negocio.	19/12/22	En proceso
		Control de actividades del Personal relacionadas con la atención y gestión de incidentes y requerimientos.	Interacción directa a través de un chat operativo, tickets REQ de reunoines	Teléfono movil,	Proactivanet	N/A	Colocar tiempo que se demora en restaurar la actividad		10 minutos	Sino se realiza en este período de tiempo, no se tiene control sobre la gestión del incidente	Periódica (cada que ocurre un evento que necesita aplicarse el SLA)	No se tiene el control de la gestión del incidente/Req/problema	Financiero:2 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 23	Plan de continuidad del negocio. Interacción directa a través de un chat operativo, tickets REQ de reunoines	19/12/22	En proceso
		Revisión de informes y reportes. (si)	Informes, email de revisión	Teléfono movil,	RADGSDM, Proactivanet	N/A	Colocar tiempo que se demora en restaurar la actividad		10 minutos	Sino se realiza en este período de tiempo, no se ejecuta el control de calidad de los informes	30 días (al finalizar cada mes)	Que la calidad de los entregables se vea degradada	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12	ACT 24	Informes, email de revisión	19/12/22	En proceso
		Evaluación de infraestructura para servicio	Correo electrónico	Computadora, teléfono movil	Proactivanet, SIEM	Luz, Internet, Telefónico	hasta 3 meses	al 3er mes	5 minutos para que el backup del SDM ejecute la actividad	Sino se realiza en este período pueden ocurrir errores en prevención que afecten la operatividad de la plataforma y por ende al servicio	6 meses	Se presente un fallo en la operación por falta de supervisión en procedimiento de evaluación preventiva	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:12 horas; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 25	RAD-PLA-GCN-09 Plan de recuperacion	19/12/22	En proceso
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Seguridad de la Información	Verificación que se haya aperturado un tickets de Incidencia/problema con prioridad alta en plataforma PROACTIVANET; y que estos hayan sido escaados a las pernas correspondientes.	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	Computador Plataforma ProactivaNet	ProactivaNet Correo electrónico	Energia eléctrica	- 10 min hasta revisar el tickets una vez haya información de la situación. - 1Hra. Aprox. en pérdida de información hasta que el área operativa controle la situación.	Tiempo de espera máxima de pérdida de información mientras el área operaciones controle la situación	1 Horas	Tiempo de respuesta de recuperación sin causar daño estando inactivo el servicio.		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Financiero:24 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:8 horas; - Objetivos del negocio:1 mes	ACT 26	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	19/12/22	En proceso
		Recibe respuesta de las acciones tomadas por parte del Área de Operaciones (incluido el equipo de CSIRT), referente al tratamiento del incidente informado. -Si las acciones fueron efectivas se incluye dicha información diligenciando a través de plataforma PROACTIVANET - Atención de incidente de seguridad informática para cerrar el incidente.	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	Computador Telefono movil	Correo electrónica, Plataforma ProactivaNet	Energia electrica Internet	30 min mientras se coordine la validación de que la situación haya sido controlado	Tiempo de espera máxima de pérdida de información mientras se valide/coordine la certeza del control de la situación	1 Horas	Tiempo de respuesta de recuperación sin causar daño estando inactivo el servicio.		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:1 mes	ACT 27	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	19/12/22	En proceso
		Reporta al Gerente General el incidente de seguridad informática ocurrido y las acciones tomadas para mitigar y/o corregir sus implicaciones.	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	Computador Telefono movil	Correo electrónica, Plataforma ProactivaNet	Energia electrica Internet	30 min una vez validado que la situacion haya sido controlado.	Tiempo de espera máxima una vez hayan informado y validado a cerca del control de la situación para la emisión del Informe de Crisis.	1 Horas	Tiempo de respuesta de recuperación sin causar daño estando inactivo el servicio.		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 28	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	19/12/22	En proceso
		Comunica las decisiones respectivas sobre otras implicaciones del incidente de seguridad informática e inicia las actividades de coordinación con el Área Administrativa para realizar las acciones correspondientes, como, por ejemplo, verificar si la acción tiene implicaciones disciplinarias y/o penales.	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	Computador Telefono movil	Correo electrónica, Plataforma ProactivaNet	Energia electrica Internet	N/A	N/A	1 Horas	Tiempo de respuesta de recuperación sin causar daño estando inactivo el servicio.		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 29	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	19/12/22	En proceso
		Archiva los documentos e información asociada al incidente de seguridad informática.	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	Computador Telefono movil	Correo electrónica, Plataforma ProactivaNet	Energia electrica Internet	N/A		1 Horas	Tiempo de respuesta de recuperación sin causar daño estando inactivo el servicio.		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes	ACT 30	Procedimiento atención de Incidentes de Seguridad Informática Solicitud de Tickets	19/12/22	En proceso
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de	Infraestructura	Monitoreo de la infraestructura tecnológica	Registro revisión de la salud de infraestructura	Computadora Celulares Internet	Zabbix PRTG Hojas de electronica Internet	Energia Eléctrica / agua	2	El monitoreo de consumo de recursos de los sistemas de información puede tener una perdida de información de 2 horas, mientras se recupera la información del respaldo	4	Tiempo que se demora en restaurar la máquina virtual que contiene el aplicativo zabbix, PRTG.	6	El no realizar monitoreo de la infraestructura, no se podría determinar el estado de salud de los diferentes servicios lo que causaría no tener datos para la elaboración de los informes de cumplimiento de SLA.	Financiero:4 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 31	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado

MATRIZ DE ANALISIS DEL IMPACTO DEL NEGOCIO (BIA)

Fecha de emisión		Código de documento	Nivel de confidencialidad
1/2/23		RAD-REG	RESTRINGIDO

seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.		Obtención de respaldos de información	VEEAM (Registros automatiza de respaldos) Acronis (Herramienta de respaldo de correo electronico. Registro de verificación de respaldos y pruebas	Computadora Servidor virtual Internet	VEEAM Acronis Internet	Energía Eléctrica / agua	1	Obtención de respaldos de los sistemas y servicios puede tener una perdida de información de 1 hora.	2	Tiempo que se demora en retaurar el sistema de obtención de respaldos, VEAMM y Acronix	3	Al no contar con los respaldos de la información causaría pérdida de credibilidad y problemas legales	Financiero:12 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 32	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
-Diversidad de equipos integrados . - Recolección, retención de logs. - Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Gestión de TI Interno & Service Desk	Gestión de Incidentes de TI Atención de Tickets de TI	Matriz registro de mantenimiento y Service Desk	Discos duros externos de respaldo Computadora Internet	Procativanet Hoja de electrónica	Energía Eléctrica	1	Segundo nivel de soporte técnico dentro del escalamiento de la gestión de incidentes	2	Tiempo que tome en restaurar el servidor y servicio de proactivanet	3	Se extiende el tiempo de entrega de los informes de atención a los tickets realizados	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:2 dias; - Contractual:2 dias; - Objetivos del negocio:1 mes	ACT 33	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
		Inventario de equipos (Gestión de activos de TI)	MAtriz de inventario	Computadora	Hoja Electrónica	Energía Eléctrica	4	Inventario de Equipos	4	Tiempo que tome aen actualizar el inventario	4	Perdida de información del inventario de equipos de Tecnologáia	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 34	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
		Realizar cambios en la Configuración	Matriz de configuraciones	Computadora	Hoja Electrónica	Energía Eléctrica	4	Inventario de Configuraciones	4	Tiempo que tome en volver a generar el inventario de configuraciones	4	Perdida de informaciónde las configuraciones de los equipos de grupo radical y de clientes	Financiero:8 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:24 horas; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 35	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
		Administrar los cambios en la infraestructura de TI	Matriz de cambios	Computadora	Hoja Electrónica	Energía Eléctrica	4	Inventario de cambios	4	Se puede perder datos de cambios ralizados	4	Perdidad de información de los cambios realizados	Financiero:8 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 36	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
		Administrar la capacidad de TI	Matriz de capacidad de infraestructura	Computadora	Hoja Electrónica	Energía Eléctrica	4	Inventario de recursos consumidos y disponibles	4		4	No contar con recursos tecnológicos para nuevos proyectos	Financiero:4 horas; - Imagen y Reputación :1 horas; - Legal o regulatorio:5 hora; - Contractual:8 hora; - Objetivos del negocio:24 horas	ACT 37	Plan de recuperación ante desastres tecnológicos (DRP)	19/12/22	Gestionado
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. - Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Gestión de la continuidad	Análisis de riesgos	Plan de emergencia y contingencia Plan de continuidad del negocio	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Correo electronico Hojas de electronica	Energía Eléctrica / agua	1	Tiempo que puedo esperar para la gestión de análisis de riesgos	1	Tiempo para reanudar el análisis de riesgos	1	Daño en la infraestructura física de la oficina.	Financiero:8 horas; - Imagen y Reputación :1mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 38	Plan de continuidad del negocio.	19/12/22	Gestionado
		Recuperación ante desastres	Plan de recuperación ante desastres tecnológicos	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Correo electronico Hojas de electronica	Energía Eléctrica / agua	1	Tiempo que puedo esperar para la gestión de recuperación ante desastres	4	Tiempo que tome en la recuperación ante desastres	8	Indisponibilidad de servicios de TI	Financiero:2 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 39	Plan de continuidad del negocio.	19/12/22	Gestionado
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Gestión de compras	Recibir requerimiento de compra del área administrativa	Solicitud y orden de compra	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Correo electronico Hojas de electronica	Energía Eléctrica / agua	8	Tiempo que puedo esperar para recibir el requerimiento de compras.	8	Tiempo para reanudar la actividad	24	Desconocimiento de la necesidad de requerimiento para la adquisición de equipos, insumos, soluciones informáticas o contratar servicios de terceros	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 40	Plan de continuidad del negocio	19/12/22	Gestionado
		Compras	Ordenes de compra, formatos para evalución de proveedores, inscripción de proveedores.	Computador portatil asistente administrativo J21 - Servidor al que estna conectados internet-computador director financiero	Excel, word, FINETIME	Microsoft office Energía electrica	Depende del acceso al servidor	Tiempo que puedo esperar para realizar las compras	2 minutos	Tiempo en restaurar la compras	24	No poder realizar las compras y servir a los clientes	Financiero:8 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 41	Plan de continuidad del negocio	19/12/22	Gestionado
		Envia órdenes de compra técnica y adminstivas al proveedor batrave de mails	Orden de compra	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Correo electronico	Energía Eléctrica / agua	2	Tiempo que puedo esperar para enviar la órden de compra al proveedor.	1	Tiempo para reanudar el envio de la órden de compra al proveedor	6	Demora en la entrega de los productos solicitados al proveedor.	Financiero:8 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 42	Plan de continuidad del negocio	19/12/22	Gestionado
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Gestión de Talento Humano	Aperturar la convocatoria interna o externa de acuerdo al caso.	Publicaciones de la oferta laboral	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora Publicaciones de la o las vacantes a ser cubiertas.	Plataformas digitales	Energía Eléctrica / agua	72	Tiempo de espera en aperturar la ofeta laboral.	120	Tiempo máximo que puedo esperar para recuperar el no haber realizado la actividad.	192	No tener candidatos para la selección de personal requerido.	Financiero:12 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 43	Plan de continuidad del negocio	19/12/22	Gestionado
		Seleccionar al personal a cubrir la vacante.	Hoja de vida	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Correo electronico	Energía Eléctrica / agua	48	Tiempo para la entrega de la hoja de vida despues de la contratación.	72	Tiempo máximo que puedo esperar para la selección del personal.	120	Contratación de personal no competente para el área solicitada.	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 44	Plan de continuidad del negocio	19/12/22	Gestionado
		Capacitación de personal	Certificaciones	Computador portatil gerente administrativo fianciero - Computador portatil asistente administrativo Servidor al que estan conectados internet- computador director financiero	Excel, word, FINETIME	Microsoft office Energía electrica	Depende del acceso al servidor	Tiempo para la realización de las capacitaciones	4	Tiempo máximo que puedo esperar para realizar la capitación	24 horas	No tener acceso a las capacitaciones	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 45	Plan de continuidad del negocio	19/12/22	Gestionado
		Realizar las evaluaciones de desempeño del personal antiguo (anual).	Evaluación anual desempeño	Espacio Físico, incluyendo sillas y mesas. PC/Laptop, con acceso a internet. Impresora	Hojas de electronica Correo electronico	Energía Eléctrica / agua	48	Tiempo sin realizar la evaluación de desempeño al personal antiguo.	1	Tiempo requerido para realizar la evaluación de desempeño al personal antiguo.	4	No tener una retroalimentación de la competencia del personal en los diferentes ámbitos	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes	ACT 46	Plan de continuidad del negocio	19/12/22	Gestionado
-Diversidad de equipos integrados . - Recolección, retención de logs. -Análisis de logs y monitoreo de eventos de seguridad. -Identificación de amenazas de seguridad. -Gestión de incidentes y reportes. -Reacción ante amenazas -Control ante amenazas -Soluciones con medidas preventivas.	Marketing e imagen corporativa	Selección de contenido de tendencias de ciberseguridad para redes sociales.	Bitacora de información	Computador, teléfono móvil	Google, twitter Internet	Energia electrica Internet Empresa Eléctrica Quito	0,5	0,5 minutos en retomar la selección de contenido de tendencias de ciberseguirda para redese sociales	0,15	0,15 minutos en recuperar la actividad sin causar un daño significativo a la empresa	3 horas (disponibilidad del servicio) como tiempo máximo de interrupción	Pérdida de credenciales que afectarian la credibilidad con la información pública	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 47	Plan de continuidad del negocio	19/12/22	Gestionado
		Coordinación y desarrollo de presentaciones y comunicaciones	Plantillas con formato Archivos contenido desarrollado fuentes de la nube	Computador, documentos fuente	Office 365, programas de diseño, Internet, Google	Energia electrica Internet Empresa Eléctrica Quito	1	1 hora en ubicar los contenidos y archivos para generar las ppt	0,45	45 minutos en recuperar la actividad sin causar un daño significativo a la empresa	3 horas (disponibilidad del servicio) como tiempo máximo de interrupción	Pérdida de los archivos	Financiero:2 días; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas	ACT 48	Plan de continuidad del negocio	19/12/22	Gestionado

Tipos y nivel de impactos según categoría

Tipos de impacto	Detalle del tipo de impacto	Nivel de impacto	Puntaje	Descripción
	Pérdidas financieras debido a	Muy bajo	1	Se considera un impacto de nivel muy bajo hasta 100 mil Usd

	MATRIZ DE ANALISIS DEL IMPACTO DEL NEGOCIO (BIA)				
	Fecha de emisión			Código de documento	Nivel de confidencialidad
	1/2/23			RAD-REG	RESTRINGIDO

Financiero (facturación)	multas, sanciones, pérdida de beneficios o disminuyen la cuota de Mercado.	Bajo	2	Se considera un impacto de nivel bajo hasta 250 mil Usd
		Medio	3	Se considera un impacto de nivel medio hasta 500 mil Usd
		Alto	4	Se considera un impacto de nivel alto hasta 1,5 millones Usd
		Muy alto	5	Se considera un impacto de nivel muy alto, mayor a 1 millones Usd
Imagen y Reputación	Opinión negativa o daños a la marca	Muy bajo	1	Se considera un nivel muy bajo si: El impacto no afecta la imagen de la empresa. Hasta 5 clientes finales afectados
		Bajo	2	Se considera un nivel bajo si: El impacto afecta levemente la imagen de la empresa. Hasta 15 clientes finales afectados
		Medio	3	Se considera un nivel medio si: El impacto afecta la imagen de la empresa. Hasta 30 clientes finales afectados
		Alto	4	Se considera un nivel alto si: El impacto afecta en gran medida la imagen de la empresa. Hasta 40 clientes finales afectados
		Muy alto	5	Se considera un nivel muy alto si: El impacto afecta gravemente la imagen de la empresa. Más de 50 clientes finales afectados
Legal o regulatorio	Responsabilidades litigiosas y retiro de la licencia para el comercio	Muy bajo	1	Amonestaciones leves a la organización por parte del IESS, Ministerio de Trabajo, SRI, Municipio de Quito, Ministerio de Gobierno u otros (Hasta 0,2 SBU)
		Bajo	2	Amonestaciones leves a la organización por parte del IESS, Ministerio de Trabajo, SRI, Municipio de Quito, Ministerio de Gobierno u otros. (Hasta 0,4 SBU)
		Medio	3	Amonestaciones leves a la organización por parte del IESS, Ministerio de Trabajo, SRI, Municipio de Quito, Ministerio de Gobierno u otros (Hasta 0,6 SBU)
		Alto	4	Amonestaciones graves a la organización por parte del IESS, Ministerio de Trabajo, SRI, Municipio de Quito, Ministerio de Gobierno u otros. Suspensión de licencia de funcionamiento de la empresa. Suspensión de la entrega de un producto o servicio de la empresa. (Hasta 0,8 SBU)
		Muy alto	5	Amonestaciones graves a la organización por parte del IESS, Ministerio de Trabajo, SRI, Municipio de Quito, Ministerio de Gobierno u otros. Cancelación de licencia de funcionamiento de la empresa. Cancelación de la entrega de un producto o servicio de la empresa. Intervención de la empresa o sometimiento a régimen de vigilancia. (1 SBU)
Contractual	Incumplimiento de contratos y obligaciones entre las organizaciones	Muy bajo	1	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta 25 mil Usd)
		Bajo	2	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta 50 mil Usd)
		Medio	3	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta 80 mil Usd)
		Alto	4	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (Hasta 120 mil Usd)
		Muy alto	5	Incumplimiento de cláusulas contractuales con proveedores o clientes con posibilidad de demandas. (150 mil Usd)
Objetivos del negocio	Si no se cumplan los objetivos fijados o tomar ventaja de las oportunidades	Muy bajo	1	Incumplimiento en los objetivos que generen un impacto muy bajo en la empresa. (nivel de impacto 6)
		Bajo	2	Incumplimiento en los objetivos que generen un impacto bajo en la empresa. (nivel de impacto 12)
		Medio	3	Incumplimiento en los objetivos que generen un impacto medio en la empresa. (nivel de impacto 18)
		Alto	4	Incumplimiento en los objetivos que generen un impacto alto en la empresa. (nivel de impacto 24)
		Muy alto	5	Incumplimiento en los objetivos que generen un impacto muy alto en la empresa. (nivel de impacto 32)

DETERMINACIÓN DE RPO, RTO, MTPD

Conceptos:

RPO (Recovery Point Objetive): El punto objetivo de recuperación. Hace referencia a la cantidad de información que la empresa está dispuesta a perder ante algún incidente que amenace la continuidad de sus operaciones. Para determinar el valor de este parámetro, con los dueños de los procesos, se identificó el lugar de almacenamiento de la información que se gestiona en cada proceso, a efectos de determinar la frecuencia con la que se realiza el backup a las bases de datos y servidores que almacenan dicha información.

RTO (Recovery Time Objetive): El tiempo objetivo de recuperación. Es el tiempo que tiene una organización para poder reanudar sus operaciones y continuar brindando el producto o servicio afectado. El RTO se calcula simulando la ejecución de un proceso considerando la ausencia de principales factores tales como, personal clave, sistemas sobre los cuales se soporta las operaciones, proveedores importantes y similares.

MTPD (Máximum Tolerable Period of Disruption): El periodo máximo de interrupción tolerable está referido al tiempo máximo que tiene la organización para tener inoperativo sus negocios, antes de que dicha inoperatividad comience a generar pérdidas graves para la empresa, y pongan en riesgo la continuidad de la misma. Para poder establecer el MTPD, se debe tener en cuenta el apetito al riesgo definido por la empresa. Para establecer dicho apetito, la organización ha considerado los cinco tipos de impacto cuantificables: Financiero, Imagen y Reputación, Legal o regulatorio, Contractual, Objetivos del negocio.

Data para determinación del RPO, RTO, MTPD

REFERENCIA	PROCESO	RIESGO	Tipo de impacto	Periodo máximo de interrupción tolerable																				MTPD BIA
				0,25 h	0,5 h	1 hr	2 hr	3 hr	4 hr	5 hr	6 hr	7 hr	8 hr	12 hr	18 hr	24 hr	2 día	3 días	5 días	7 días	11 días	1 mes	MTPD	
1	Gestión de la Dirección	No contar con la representación legal y judicial para la firma de documentos legales. Causaría insertidumbre en las partes interesadas	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	5	--	--	--	--	3 días	Financiero:3 días; - Imagen y Reputación :24 horas; - Legal o regulatorio:2 días; - Contractual:3 días; - Objetivos del negocio:3 días
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	3	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	3	--	--	--	--	--	2 días	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	3 días	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	3 días	
2	Planeación Financiera	* Riesgo de pérdida de información que se encuentra en el servidor. * Riesgo de demora en pago y cobros por imposibilidad de ingreso a las plataformas de las intituciones financieras	Financiero	--	--	--	2		--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :4 horas; - Legal o regulatorio:0,5 horas; - Contractual:0,5 horas; - Objetivos del
			Imagen y Reputación	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	
			Legal o regulatorio	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	0,5 horas	
			Contractual	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	0,5 horas	
			Objetivos del negocio	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	0,25 horas	
3		* Riesgo de incumplimiento de obligaciones tributarias, laborales y societarias * Riesgo de imposibilidad de supcripcion de contratos nuevos	Financiero	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	Financiero:1 hora; - Imagen y Reputación :1 hora; - Legal o regulatorio:4 horas; - Contractual:1 hora; - Objetivos del negocio:1 hora
			Imagen y Reputación	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Legal o regulatorio	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	
			Contractual	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Objetivos del negocio	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
4	Sistema Integrado de Gestión	Demoras de acuerdo a la planificación de implementación de los sistemas de gestión.	Financiero	--	--	--	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	Financiero:4 horas; - Imagen y Reputación :2 horas; - Legal o regulatorio:1 horas; - Contractual:12 horas; - Objetivos del negocio:24 horas
			Imagen y Reputación	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	
			Legal o regulatorio	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	12 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	24 horas	
5		Demoras de acuerdo a la planificación de mangtenimiento de los sistemas de gestión.	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	N/A	Financiero:N/A; - Imagen y Reputación : 6 horas; - Legal o regulatorio:N/A; - Contractual:6 horas; - Objetivos del negocio:1 horas
			Imagen y Reputación	--	--	--	--	--	--	--	4	--	--	--	--	--	--	--	--	--	--	--	6 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	N/A	
			Contractual	--	--	--	--	--	--	--	4	--	--	--	--	--	--	--	--	--	--	--	6 horas	
			Objetivos del negocio	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 horas	
	Estrategia, Monitorizacion y	No contar con información actualizada sobre las	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	N/A	Financiero:N/A; - Imagen y Reputación :4 horas; - Legal o
			Imagen y Reputación	--	--	--	--	4	--	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	

6	Control de Ventas	oportunidades cuando haya ausencia del personal a cargo	Legal o regulatorio	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:N/A
			Contractual	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	N/A	
7	Gestión de acuerdo con proveedores	Perder beneficios comerciales al no registrar a tiempo la oportunidad	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	N/A	Financiero:N/A; - Imagen y Reputación :4 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:2 horas
			Imagen y Reputación	--	--	--	--	4	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	
			Legal o regulatorio	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Contractual	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	2 horas	
8	Comercial	No alcanzar a presentar ofertas en el portal	Financiero	--	--	--	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	Financiero:4 horas; - Imagen y Reputación :1 horas; - Legal o regulatorio:5 hora; - Contractual:8 hora; - Objetivos del negocio:24 horas
			Imagen y Reputación	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 horas	
			Legal o regulatorio	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	5 hora	
			Contractual	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	8 hora	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
9		No alcanzar a presentar ofertas en el portal	Financiero	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :1 hora; - Legal o regulatorio:8 horas; - Contractual:1 hora; - Objetivos del negocio:24 horas
			Imagen y Reputación	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
10		No se pudo participar en la propuesta.	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :3 horas; - Legal o regulatorio:1 hora; - Contractual:1 hora; - Objetivos del negocio:1 mes
			Imagen y Reputación	--	--	--	--	4	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	3 horas	
			Legal o regulatorio	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Contractual	--	--	1	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
11	Gestión Integrada de Proyectos	No se puede iniciar el proceso de planificación del proyecto No se puede realizar la reunión de kickoff del	Financiero	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	Financiero:4 horas; - Imagen y Reputación :8 horas; - Legal o regulatorio:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	8 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	12 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1 mes	
12		No iniciar en las fechas estipuladas contractualmente	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1 mes	Financiero:1 mes; - Imagen y Reputación :11 días; - Legal o regulatorio:1 mes; - Contractual:11 días; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	11 días	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	11 días	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
13		No cumplir con las fechas de la planificación del proyecto	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 mes	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 mes	
14		No cumplir con las fechas de la ejecución del proyecto	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :11 días; - Legal o regulatorio:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	11 días	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 mes	
15		No cumplir con las fechas de la ejecución del proyecto	Financiero	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :7 días; - Legal o regulatorio:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	7 días	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	24 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 mes	
			Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :1 mes; - Legal o
			Imagen y Reputación	--	--	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	

16	Ciberseguridad	Cambio de recurso con pedido de prórroga y multa	Legal o regulatorio	--	--	--	--	--	--	--	--	--	2	--	--	2	--	--	--	--	--	--	8 horas	regulatorio:8 horas; - Contractual:24 horas; - Objetivos del negocio:1 mes
			Contractual	--	--	--	--	--	--	--	--	--		--	--	2	--	--	--	--	--	--	24 horas	
			Objetivos del negocio	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
17		Cambio de recurso con multa por cada hora de reetraso.	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :2 días; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	2 días	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
18		Cambio de recurso con multa por cada hora de reetraso.	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:1 mes; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
19	SOC CSIRT	Incumpliento del SLA y del servicio contratado por los clientes	Financiero	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :8 horas; - Legal o regulatorio:24 horas; - Contractual:24
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	24 horas	
			Contractual	--	--	--	--	--	--	--	--	--	2	--	--	2	--	--	--	--	--	--	24 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
20	Servicio Posventa	Se puede obviar problemas que afectan los SLA	Financiero	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :4 horas; - Legal o regulatorio:1 hora; - Contractual:8 horas; -
			Imagen y Reputación	--	--	--	--	--	2	--	--	--	--	--	--	1	--	--	--	--	--	--	4 horas	
			Legal o regulatorio	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1 hora	
			Contractual	--	--	--	--	--	--	--	--	--	2	--	--	2	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
21		Se puede obviar problemas que afectan los SLA	Financiero	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	Financiero:4 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:2 horas; - Contractual:12
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 hiras	
22		Ejecución de multas por incumplimiento SLA	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	24 horas	Financiero:24 horas; Imagen y Reputación :12 horas; - Legal o regulatorio:12 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
23		No se tiene el control de la gestión del incidente/Req/problema	Financiero	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
24		Que la calidad de los entregables se vea degradada	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
25		Se presente un fallo en la operación por falta de supervisión en procedimiento de evaluación preventiva	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:12 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	12 horas	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
26		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:8 horas; - Objetivos del negocio:1 mes
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	

27	Seguridad de la Información	Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar l s acc ones	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:1 mes
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	1	1 mes	
28		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
29		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
30		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; - Objetivos del negocio:12 horas
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
31	Infraestructura	El no realizar monitoreo de la infraestructura, no se podría determinar el estado de salud de los diferentes servicios lo que causaría no tener datos para la elaboración de los informes de cumplimiento de SLA.	Financiero	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	--	--	--	--	4 horas	Financiero:4 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del negocio:1 mes
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
32		Al no contar con los respaldos de la información causaría pérdida de credibilidad y problemas legales	Financiero	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	12 horas	Financiero:12 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:1 mes; - Contractual:1 mes; - Objetivos del
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
33	Gestión de TI Interno & Service Desk	Se extiende el tiempo de entrega de los informes de atención a los ticktes realizados	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:2 días; - Contractual:2 días; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	2 días	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	2	--	--	--	--	--	2 días	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	
34		Perdida de información del inventario de equipos de Tecnologáía	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; - Imagen y Reputación :1 mes; - Legal o regulatorio:1 mes; - Contractual:7 días; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	7 días	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
35		Perdida de informacióndе las configuraciones de los equipos internos y de clientes	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; - Imagen y Reputación :24 horas; - Legal o regulatorio:8 horas; - Contractual:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	
36		Perdidad de información de los cambios realizados	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; - Imagen y Reputación :1 mes; - Legal o regulatorio:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	24 horas	
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	

37		No contar con recursos tecnológicos para nuevos proyectos	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	:1 mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
38	Gestión de continuidad	Daño en la infraestructura física de la oficina.	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	:1mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
39		Indisponibilidad de servicios de TI	Financiero	--	--	--	3	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2 horas	Financiero:2 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	:1 mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
40	Gestión de compras	Desconocimiento de la necesidad de requerimiento para la adquisición de equipos, insumos, soluciones informáticas o	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	:24 horas; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	regulatorio:8 horas; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	Contractual:8 horas; -
41		No poder realizar las compras y servir a los clientes	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	:24 horas; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
42		Demora en la entrega de los productos solicitados al proveedor.	Financiero	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	--	8 horas	Financiero:8 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	:24 horas; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
43	Talento Humano	No tener candidatos para la selección de personal requerido.	Financiero	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	--	--	--	12 horas	Financiero:12 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	2	1 mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	:1 mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	1 mes	Contractual:1 mes; -
44		Contratación de personal no competente para el área solicitada.	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	7 días	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	:7 días; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
45		No tener acceso a las capacitaciones	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	2	1 mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	:1 mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	2	1 mes	Contractual:1 mes; -
46		No tener una retroalimentación de la competencia del personal en los diferentes ámbitos	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	2	1 mes	Financiero:1 mes; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	2	1 mes	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	:1 mes; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	2	1 mes	regulatorio:1 mes; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	1 mes	Contractual:1 mes; -
47	Marketing e imagen corporativa	Pérdida de credenciales que afectarian la credibilidad con la información pública	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Financiero:24 horas; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	:24 horas; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	regulatorio:8 horas; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	Contractual:8 horas; -
48		Pérdida de los archivos	Financiero	--	--	--	--	--	--	--	--	--	--	--	--	--	2	--	--	--	--	--	2 días	Financiero:2 días; -
			Imagen y Reputación	--	--	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	24 horas	Imagen y Reputación
			Legal o regulatorio	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	:24 horas; - Legal o
			Contractual	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	--	8 horas	regulatorio:8 horas; -
			Objetivos del negocio	--	--	--	--	--	--	--	--	--	--	1	--	--	--	--	--	--	--	--	12 horas	Contractual:8 horas; -

Origen de la estrategia	Proceso	Riesgo	Estrategia de continuidad	Descripción	Ventajas	Desventajas	a) Cumple los requisitos para continuar y recuperar las actividades prioritarias dentro de los plazos identificados y la capacidad acordada.	b) Protege las actividades prioritarias de la organización.	c) Reducen la probabilidad de interrupción.	d) Acorta el periodo de interrupción.	e) Limita el impacto de la interrupción en los productos y servicios de la organización.	f) Garantiza la disponibilidad de recursos adecuados.	Respuesta de la estrategia a la temporalidad de la			Selección de estrategias y			Recursos
													Antes	Durante	Después	a) Cumple los requisitos para continuar y recuperar las actividades prioritarias dentro de los plazos identificados y la capacidad acordada;	b) Considera la cantidad y el tipo de riesgo que la organización puede o no asumir	c) Considera los costes y beneficios asociados.	
Análisis del impacto del negocio	Gestión de la Dirección	No contar con la representación legal y judicial para la firma de documentos legales. Causaría insertidumbre en las partes interesadas	La representación legal de acuerdo a los estatutos de la empresa en ausencia del gerente general el presidente asumira la responsabilidad	Contar en todo momento con la representación legal para diferentes tramites legales	Representación legal constante		si	si	si	si	si	si	X			si	si	no	a) Personas: Junta de socios b) Información y datos: Estrituras de constitución de la empresa c) Infraestructura física: Estación de trabajo d) Equipos y consumibles: Computador portatil, proyector. e) Sistemas de TIC: Telefonía, correo electronico, internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Asesor externo
Análisis del impacto del negocio	Planeación Financiera	* Riesgo de pérdida de información que se encuentra en el servidor. * Riesgo de demora en pago y cobros por imposibilidad de ingreso a las plataformas de las intituciones financieras	* Conexión al sistema contable desde cualquier lugar * Mantener los archivos administrativos finanancieros en la nube para facil acceso	* Al acceder al sistema contable desde cualquier lugar se puede ingresar y consultar la información desde cualquier lugar. * La información se encuentra almacenada en una sola carpeta compartida Administrativo Financiero para facil acceso de los usuarios	Acceso e ingreso a y de la información	No se pueden imprimir los documentos físicos y el archivo físico queda retrasado	si	si	si	si	si	si	X			si	si	no	a) Personas: auxiliar contable, contador, gerente financiero b) Información y datos: Comprobantes de venta y/o retenciones (compras y ventas) c) Infraestructura física: Computadores portatiles asistente, contador y financieros d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet f) Transporte y logística: N/A g) Finanzas: Fondos en bancos para pagos h) Socios y proveedores: Clientes y/o proveedores

Análisis del impacto del negocio		* Riesgo de incumplimiento de obligaciones tributarias, laborales y societarias * Riesgo de imposibilidad de supcripcion de contratos nuevos	* Mantener los archivos administrativos finanancieros en la nube para facil acceso * Mantener accesos en línea a los bancos para los pagos.	* La información se encuentra almacenada en una sola carpeta compartida Administrativo Financiero para facil acceso de los usuarios. * Los controles se pueden realizar a traves de los correos y chats	Mantener acceso a la infromación	No se pueden imprimir los documentos físicos y el archivo físico queda retrasado	si	si	si	si	si	si	X			si	si	no	a) Personas: auxiliar contable, contador, gerente financiero, asitente administrativo, director financiero. b) Información y datos: Archivos generados para control c) Infraestructura física: oficina d) Equipos y consumibles: Computadores e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: Fondos en bancos para pagos h) Socios y proveedores: Clientes y/o proveedores
Análisis del impacto del negocio	Sistema Integrado de Gestión	Demoras de acuerdo a la planificación de implementación de los sistemas de gestión.	Seguimiento constante al programa de actividades	Verificación constante de programa de actividades	Cumplimiento de actividades en los tiempos planificados	No contar con tiempo para realizar el seguimiento constante	si	si	si	si	si	si	X			si	si	no	a) Personas: Coordinador del SIG b) Información y datos: Programa de actividades c) Infraestructura física: estación de trabajo d) Equipos y consumibles: Computadores e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A
Análisis del impacto del negocio		Demoras de acuerdo a la planificación de mantenimiento de los sistemas de gestión.	Contar con personal o empresa externa que realice el seguimiento al mantenimiento de los sistemas de gestión	Mantenimiento constante a los sistemas de gestión	Información actualiza	La persona encargada del mantenimiento no tenga tiempo para realizar el seguimiento	si	si	si	si	si	si	X			si	si	no	a) Personas: Coordinador del SIG b) Información y datos: Programa de actividades c) Infraestructura física: estación de trabajo d) Equipos y consumibles: Computadores e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Asesor externo
Análisis del impacto del negocio	Estrategia, Monitorizacion y Control de Ventas	No contar con información actualizada sobre las oportunidades cuando haya ausencia del personal a cargo	Seguimiento constate al registro de oportunidades	La dirección Comercial semanalmente generará el reporte del registro de oportunidades en el CRM	Mantener información actualizada	Falta de tiempo para realizar el seguimiento	si	si	si	si	si	si	X			si	si	no	a) Personas: Directora Comercial b) Información y datos: Reporte del CRM c) Infraestructura física: Oficina d) Equipos y consumibles: Computador e) Sistemas de TIC: Plataforma CRM e internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet
Análisis del impacto del negocio	Gestión de acuerdo con proveedores	Perder beneficios comerciales al no registrar a tiempo la oportunidad	Evidenciar el registro de oportunidades en una matriz de seguimiento	La asistente Comercial registrará en el menor tiempo posible la aprobación del registro de oportunidades en la matriz de seguimiento	Mantener información actualizada	Falta de tiempo para realizar el seguimiento	si	si	si	si	si	si	X			si	si	no	a) Personas: Asistente Comercial b) Información y datos: Mail de partner c) Infraestructura física: Oficina d) Equipos y consumibles: Computador e) Sistemas de TIC: Portales de partner f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Puntonet

Análisis del impacto del negocio	Comercial	No alcanzar a presentar ofertas en el portal	Detectar a tiempo una oferta en el portal Sercop	El asistente comercial revise constante el portal Sercop	Conocimiento de requerimientos de ofertas	El asistente comercial no cuente con tiempo para revisar el portal	si	si	si	si	si	si	X			si	si	no	a) Personas: Director Comercial, Asistente Comercial b) Información y datos: Portal Sercop c) Infraestructura física: Estación de trabajo d) Equipos y consumibles: Computador portatil e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Puntonet
Análisis del impacto del negocio		No alcanzar a presentar ofertas en el portal	Prepar a tiempo una oferta para subir al portal	Contar con tiempo suficiente para poder prepara las documentación solicitada en la oferta	Envio de ofertas en los tiempos establecidos con toda la documentación de respaldo	Envio de ofertas sin los respaldos solicitados por falta de tiempo de la persona encargada de subir las ofertas	si	si	si	si	si	si	X			si	si	no	a) Personas: Director Comercial, Asistente Comercial b) Información y datos: Portal Sercop c) Infraestructura física: Estación de trabajo d) Equipos y consumibles: Computador portatil e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Puntonet
Análisis del impacto del negocio		No se pudo participar en la propuesta	Participar en las subastas	Poder realizar preguntas en la subasta			si	si	si	si	si	si	X			si	si	no	a) Personas: Director Comercial, Asistente Comercial b) Información y datos: Portal Sercop c) Infraestructura física: Estación de trabajo d) Equipos y consumibles: Computador portatil e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Puntonet
Análisis del impacto del negocio		No se puede iniciar el proceso de planificación del proyecto No se puede realizar la reunión de kickoff del proyecto	Envío de documentación completa	Normar documetación a entregar por parte del Area Comercial	Tener documentaciómn completa para ejecutar el proyecto	Poner en riesgo la ejecución del proyecto en plazos y en entregables	si	si	si	si	si	si	X			si	si	no	a) Personas: Director de Proyectos y Directora Comercial b) Información y datos: Documentación del contrato c) Infraestructura física: oficina d) Equipos y consumibles: Computadora e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet
Análisis del impacto del negocio		No iniciar en las fechas estipuladas contractualmente	Asignar a Director el proyecto	Dirigir el proyecto el mismo Director de Proyectos sin designar a un PM	Iniciar el proyecto a tiempo	Mas carga laboral	si	si	si	si	si	si	X			si	si	no	a) Personas: Director de Proyectos y Directora Comercial b) Información y datos: c) Infraestructura física: oficina d) Equipos y consumibles: Computadora e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet

Análisis del impacto del negocio	Gestión Integrada de Proyectos	No cumplir con las fechas de la planificación del proyecto	Planificación virtual por llamada telefónica	Planificar vía telefónica y generar acta de reunión para posterior envío por correo electrónico.	Realizar la planificación a tiempo	Revisar documentos a detalle o compartir información relevante presencial o en línea	si	si	si	si	si	si	X			si	si	no	a) Personas: Director de Proyectos b) Información y datos: Calendario para agendar reuniones c) Infraestructura física: oficina d) Equipos y consumibles: Computadora e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet
Análisis del impacto del negocio		No cumplir con las fechas de la ejecución del proyecto	Ejecución virtual por llamada telefónica	Ejecutar vía telefónica y generar acta de reunión para posterior envío por correo electrónico. Solicitar tiempo adicional a los	Realizar la ejecución a tiempo	Extender en tiempo por lo que afectaría el presupuesto del proyecto.	si	si	si	si	si	si	X			si	si	no	a) Personas: Director proyectos b) Información y datos: contrato c) Infraestructura física: oficina d) Equipos y consumibles: Computadora, teléfono movil e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y
Análisis del impacto del negocio		No cumplir con las fechas de la ejecución del proyecto	Hacer llegar documentación física en las oficinas del cliente	Hacer llegar por mensajero o courier los documentos de cierre de proyecto para revisiones y firmas de aceptación.	Realizar el cierre del proyecto conforme a contrato	Robo o Perdida de documentos	si	si	si	si	si	si	X			si	si	no	a) Personas: Director proyectos b) Información y datos: contrato c) Infraestructura física: oficina d) Equipos y consumibles: Computadora, teléfono movil e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet
Análisis del impacto del negocio		Cambio de recurso con pedido de prórroga y multa.	Incrementar personal asignado para acortar tiempos	Tener al menos dos personas dependiendo el tamaño del proyecto	Redducir tiempso de implementación	Aumento de costos operativos por requerimiento de personal	si	si	si	si	si	si	X			si	si	no	a) Personas: Analista N1 (2) Analista N2 (3) b) Información y datos: Carpeta de Proyectos (Claud Sharepoint) c) Infraestructura física: Equipamiento del soporte de clientes; Laptop de especialista d) Equipos y consumibles: Impresoras, Cables, etc. e) Sistemas de TIC: Conexiones a Internet, Proactivanet; Accesos VPN, Planes de celular. f) Transporte y logística: Transporte en caso de servicio en sitio. g) Finanzas: N/A h) Socios y proveedores:Hubspot y puntonet

Análisis del impacto del negocio	Ciberseguridad	Cambio de recurso con multa por cada hora de reetraso.	Soluciones en base de backup de especialistas	Tener al menos dos personas que conozcan a soluciones implementadas, sucesiones dentro del servicio.	Mejorar la eficiencia del servicio	Aumento de costos operativos por requerimiento de personal	si	si	si	si	si	si	X			si	si	no	a) Personas: Analista N1 (2) Analista N2 (3) b) Información y datos: Carpeta de Proyectos (Claud Sharepoint) c) Infraestructura física: Equipamiento del soporte de clientes; Laptop de especialista d) Equipos y consumibles: Impresoras, Cables, etc. e) Sistemas de TIC: Conexiones a Internet, Proactivanet; Accesos VPN, Planes de celular. f) Transporte y logística: Transporte en caso de servicio en sitio. g) Finanzas: N/A h) Socios y proveedores: Hubspot y puntonet
Análisis del impacto del negocio		Cambio de recurso con multa por cada hora de reetraso.	Soluciones en base de backup de especialistas	Tener al menos dos personas que conozcan a soluciones implementadas, sucesiones dentro del servicio.	Mejorar la eficiencia del servicio	Aumento de costos operativos por requerimiento de personal	si	si	si	si	si	si	X			si	si	no	a) Personas: Analista N1 (2) Analista N2 (3) b) Información y datos: Carpeta de Proyectos (Claud Sharepoint) c) Infraestructura física: Equipamiento del soporte de clientes; Laptop de especialista d) Equipos y consumibles: Impresoras, Cables, desktop, etc. e) Sistemas de TIC: Conexiones a Internet, Proactivanet; Accesos VPN, Planes de celular. f) Transporte y logística: Transporte en caso de servicio en sitio. g) Finanzas: N/A h) Socios y proveedores: Fabricantes y Proveedores.
Análisis del impacto del negocio	SOC CSIRT	Incumpliento del SLA y del servicio contratado por los clientes	Determinacion de necesidades para contar con redundancia a nivel VPN, Software, hardware y personas.	Reducir el tiempo de recuperacion al contar con alta disponibildad en software, hardware y personas	Garantizar el servicio. Cumplimien to de SLA evitando la ejecucion de multas.	Perdida de recursos por la no utilizacion de los sistemas redundantes.	si	si	si	si	si	si	X			si	si	no	a) Personas: Analistas Nivel 1 (15), Nivel 2 (6) y coordinacion (1) b) Información y datos: Informacion y datos de proactivanet. c) Infraestructura física: Instalaciones y puntos remotos. d) Equipos y consumibles: Desktop, laptop, celular e) Sistemas de TIC: Conexion a internet, Acceso VPN y Plan de datos celular. f) Transporte y logística: g) Finanzas: h) Socios y proveedores:
Análisis del impacto del negocio		Se puede obviar problemas que afectan los SLA	Revisión del reporte generado en el sistema de la mesa de ayuda	En base a los SLA establecidos se revisa el cumplimiento de los tiempos del SLA en base a la categorización de los niveles de severidad establecidos	Contar con visibilidad de eventos que afectan el SLA para evitar en futuros periodos de servicio	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador SOC b) Información y datos: reporte SLA c) Infraestructura física: n/a d) Equipos y consumibles: computadoras e) Sistemas de TIC: Proactivanet f) Transporte y logística: n/a g) Finanzas: n/a h) Socios y proveedores: Proactivanet Nota: Recursos utilizados para llevar a cabo la estrategia

Análisis del impacto del negocio	Servicio Posventa	Se puede obviar problemas que afectan los SLA	Revisión del reporte generado en el sistema de la mesa de ayuda	En base a los SLA establecidos se revisa el cumplimiento de los tiempos del SLA en base a la categorización de los niveles de severidad establecidos	Contar con visibilidad de eventos que afectan el SLA para evitar en futuros periodos de servicio	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador SOC b) Información y datos: reporte SLA c) Infraestructura física: n/a d) Equipos y consumibles: computadoras e) Sistemas de TIC: Proactivanet f) Transporte y logística: n/a g) Finanzas: n/a h) Socios y proveedores: Proactivanet Nota: Recursos utilizados para llevar a cabo la estrategia
Análisis del impacto del negocio		Ejecución de multas por incumplimiento SLA	Revisión del reporte generado en el sistema de la mesa de ayuda	En base a los SLA establecidos se revisa el cumplimiento de los tiempos del SLA en base a la categorización de los niveles de severidad	Mantener control sobre los tiempos del SLA evitando el cobro de multas y calidad del servici	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador SOC b) Información y datos: reporte SLA c) Infraestructura física: n/a d) Equipos y consumibles: computadoras e) Sistemas de TIC: Proactivanet f) Transporte y logística: n/a g) Finanzas: n/a h) Socios y proveedores: Proactivanet
Análisis del impacto del negocio		No se tiene el control de la gestión del incidente/Req/problema	Aplciar las mejoras en otros clientes	Una vez gestionado el evento, tratar de aplicar las mejores prácticas en otros clientes	Articular las acciones para la gestión de los eventos	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador SOC, Nivel 1, Nivel 2, Director de Operaciones b) Información y datos: reporte de eventos c) Infraestructura física: n/a d) Equipos y consumibles: computadoras, teléfonos e) Sistemas de TIC: Proactivanet f) Transporte y logística: n/a g) Finanzas: n/a
Análisis del impacto del negocio		Que la calidad de los entregables se vea degradada	En cada revisión, dejar bitácora de mejoras	En base a los SLA establecidos se revisa el cumplimiento de los tiempos del SLA en base a la categorización de los niveles de severidad establecido	Optimizar tiempos	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador SOC, Nivel 1, Nivel 2, Director de Operaciones b) Información y datos: reporte de eventos c) Infraestructura física: n/a d) Equipos y consumibles: computadoras, teléfonos e) Sistemas de TIC: Proactivanet, RADGSDM f) Transporte y logística: n/a
Análisis del impacto del negocio		Se presente un fallo en la operación por falta de supervisión en procedimiento de evaluación preventiva	Revisión del reporte de la capacidad total de la infraestructura, documento remitido por el área de Infraestructura.	Esta estrategia nos servirá para supervisar las medidas preventivas y correctivas del soporte y mantenimiento de la infraestructura tecnológica para el servicio.	Contar con medidas preventivas	N/A	si	si	si	si	si	si	X			si	si	no	a) Personas: SDM, Coordinador Infraestructura b) Información y datos: Umbrales de capacidades de infraestructura tecnológica c) Infraestructura física: Oficinas UIO y lugares alternos d) Equipos y consumibles: 2 Computadoras e) Sistemas de TIC: consolas de monitoreo f) Transporte y logística: n/a g) Finanzas: n/a h) Socios y proveedores:Proveedores de

Análisis del impacto del negocio		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Activación inmediata de la Mesa de ayuda, Coordinación SOC/CSIRT/NOC y Dirección de Operaciones.	Mesa de ayuda a través de la coordinación del SOC/CSIRT/NOC y la Dirección de Operaciones deberán tomar acciones inmediatas para activar las directrices y	Actuar de manera oportuna, inmediata y eficienteme nte.	No usar los conductos o procedimientos definidos para este tipo de Incidente.	si	si	si	si	si	si	X			si	si	no	a) Personas: Mesa de Ayuda / Jill Saavedra b) Información y datos: Creación del tickets / revisión de la creación, asignación y detalles respecto al incidente. c) Infraestructura física: Garantizar los servicios activos Ingenieros de operaciones d) Equipos y consumibles: e) Sistemas de TIC: ProactivaNet activa f) Transporte y logística: N/A g) Finanzas: N/A
Análisis del impacto del negocio		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Activación inmediata de la Mesa de ayuda, Coordinación SOC/CSIRT/NOC y Dirección de Operaciones.	Mesa de ayuda a través de la coordinación del SOC/CSIRT/NOC y la Dirección de Operaciones deberán tomar acciones inmediatas para activar las directrices y procedimientos correspondientes	Actuar de manera oportuna, inmediata y eficienteme nte.	No usar los conductos o procedimientos definidos para este tipo de Incidente.	si	si	si	si	si	si	X			si	si	no	b) Información y datos: Creación del tickets / revisión de la creación, asignación y detalles respecto al incidente. c) Infraestructura física: Garantizar los servicios activos Ingenieros de operaciones d) Equipos y consumibles: e) Sistemas de TIC: ProactivaNet activa f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio	Seguridad de la Información	Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Activación inmediata de la Mesa de ayuda, Coordinación SOC/CSIRT/NOC y Dirección de Operaciones.	Mesa de ayuda a través de la coordinación del SOC/CSIRT/NOC y la Dirección de Operaciones deberán tomar acciones inmediatas para activar las directrices y procedimientos	Actuar de manera oportuna, inmediata y eficienteme nte.	No usar los conductos o procedimientos definidos para este tipo de Incidente.	si	si	si	si	si	si	X			si	si	no	a) Personas: Mesa de Ayuda / Jill Saavedra b) Información y datos: Creación del tickets / revisión de la creación, asignación y detalles respecto al incidente. c) Infraestructura física: Garantizar los servicios activos Ingenieros de operaciones d) Equipos y consumibles: e) Sistemas de TIC: ProactivaNet activa f) Transporte y logística: N/A g) Finanzas: N/A
Análisis del impacto del negocio		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Activación inmediata de la Mesa de ayuda, Coordinación SOC/CSIRT/NOC y Dirección de Operaciones.	Mesa de ayuda a través de la coordinación del SOC/CSIRT/NOC y la Dirección de Operaciones deberán tomar acciones inmediatas para activar las directrices y procedimientos	Actuar de manera oportuna, inmediata y eficienteme nte	No usar los conductos o procedimientos definidos para este tipo de Incidente.	si	si	si	si	si	si	X			si	si	no	a) Personas: Mesa de Ayuda / Jill Saavedra b) Información y datos: Creación del tickets / revisión de la creación, asignación y detalles respecto al incidente. c) Infraestructura física: Garantizar los servicios activos Ingenieros de operaciones d) Equipos y consumibles: e) Sistemas de TIC: ProactivaNet activa f) Transporte y logística: N/A g) Finanzas: N/A
Análisis del impacto del negocio		Al no registrar el ticket oportunamente y la asignación del mismo a los especialistas correspondientes, hará que no se tenga activado el equipo de respuesta de manera rápida y eficiente para tomar las acciones correspondientes.	Activación inmediata de la Mesa de ayuda, Coordinación SOC/CSIRT/NOC y Dirección de Operaciones.	Mesa de ayuda a través de la coordinación del SOC/CSIRT/NOC y la Dirección de Operaciones deberán tomar acciones inmediatas para activar las directrices y procedimientos	Actuar de manera oportuna, inmediata y eficienteme nte	No usar los conductos o procedimientos definidos para este tipo de Incidente.	si	si	si	si	si	si	X			si	si	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A

Análisis del impacto del negocio	Infraestructura	El no realizar monitoreo de la infraestructura, no se podría determinar el estado de salud de los diferentes servicios lo que causaría no tener datos para la elaboración de los informes de cumplimiento de SLA.	Tecnológica - Respaldos y Recuparación	Generar respaldos de las máquina virtual que genera el monitoreo de la infraestructura tecnológica. En caso de falla del monitoreo principal y redundante se optará por un monitoreo	Mantener un registro del estado de la infraestructura sea manual o automatizado ayuda a mantener el historio del estado de la infraestructura para la	Se requiere instalar un equipo virtual para tener redundancia del servidor de monitoreo	si	si	si	si	si	si	X			si	si	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Centro de datos virtual adicional, incremento de recursos tecnológicos en caso de ya contar con centro de datos virtual c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		Al no contar con los respaldos de la información causaría pérdida de credibilidad y problemas legales	Tecnológica - Respaldos y Recuparación	Crear una replica del almacenamiento de respaldos en centro de datos alterno en la nube.	Redundancia del almacen de respaldos	Mantener una almacen de datos de respaldos involucra costos financieros o gastos en que la empresa debe realizar.	si	si	no	no	no	si	X			si	si	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Adquisición de almacenamiento especilizado para respaldos y recuperación de información c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		Se extiende el tiempo de entrega de los informes de atención a los ticktes realizados	Sitio Alterno	Implementar redundancia en la herramienta de gestión de incidentes.	Mejorar los tiempos de entrega de los informes de atención a incidentes.	Incremento de recursos de tecnología para implementar la redundancia del aplicativo de gestión de incidentes.	si	si	si	si	no	no	X			si	no	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		Perdida de información del inventario de equipos de Tecnologáía	Mantener la información en la Nube	Los archios deben ser almacenados en la nube	Los archivos estan siempre disponibles	Incrementar recuross de almacenamiento en la nube	si	si	si	si	no	no	X			si	no	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A

Análisis del impacto del negocio	Gestión de TI Interno y Service Desk	Perdida de información de las configuraciones de los equipos internos y de clientes	Mantener la información en la Nube	Los archios deben ser almacenados en la nube	Los archivos estan siempre disponibles	Incrementar recuross de almacenamiento en la nube	si	si	si	si	no	no	X			si	no	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		Perdidad de información de los cambios realizados	Mantener la información en la Nube	Los archios deben ser almacenados en la nube	Los archivos estan siempre disponibles	Incrementar recuross de almacenamiento en la nube	si	si	si	si	no	no	X			si	no	no	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		No contar con recursos tecnológicos para nuevos proyectos	Monitoreo de los recursos existentes	Manter un monitoreo de los recursos utilizados y notificar a cada dirección la cantidad de recursos disponibles	Contar con recursos dispoibles en caso de emergencia o de nuevos proyectos	Recursos económicos para manter siempre disponible recursos tecnológicos para nuevos proyectos	Si	Si	Si	Si	Si	Si	X			Si	si	si	a) Personas: Dueño del proceso Infraestructura b) Información y datos: Incrementar los recursos tecnológicos de memoria, procesador y almacenamiento. c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio	Gestión de continuidad	Daño en la infraestructura física de la oficina.	Sitio alterno de trabajo	En estas instalaciones se debe contar con todas las aplicaciones instaladas, servidores operando adecuadamente, y estaciones de trabajo listas	Restablecimiento de las operaciones de forma inmedi	Costo elevado para la equipación de la oficina	Si	Si	Si	Si	Si	Si	X			Si	si	si	a) Personas: Dueño del proceso Continuidad del negocio b) Información y datos: Mantenimiento de la infraestructura física c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A
Análisis del impacto del negocio		Indisponibilidad de servicios de TI	Establecer planes de emergencia y contingencia ante incidentes presentados.	Establecer un plan de emergencia y contingencia para los casos en que se presente caída de todos los servicios de TI.	Disponibilidad de los servicios de TI	Ausencia de servicios de TI	Si	Si	Si	Si	Si	Si	X			Si	si	si	a) Personas: Dueño del proceso Continuidad del Negocio b) Información y datos: Plan de emergencia y contingencia c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A

Análisis del impacto del negocio	Gestión de compras	Desconocimiento de la necesidad de requerimiento para la adquisición de equipos, insumos, soluciones informáticas o contratar servicios de terceros	Requerimiento de compras con las especificaciones técnicas.	El requerimiento para la compra de equipos sea enviado por correo a la persona responsable de compras con las especificaciones técnicas.	Compra de equipos de acuerdo a los requimientos solicitados	No contar con las especificaciones técnicas de la necesidad	si	si	si	si	si	si	x			si	si	si	a) Personas: Dueño del proceso Compras b) Información y datos: Procedimiento de compras, Politica de compras c) Infraestructura física: 1 oficina d) Equipos y consumibles: laptop, e) Sistemas de TIC: Internet f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: N/A
Análisis del impacto del negocio		No poder realizar las compras y servir a los clientes	Mantener los archivos administrativos finanancieros en la nube para facil acceso * Mantener accesos en línea a los bancos para los pagos.	La información se encuentra almacenada en una sola carpeta compartida Administrativo Financiero para facil acceso de los usuarios. * Los controles se pueden realizar a traves de los correos y chats	Mantener acceso a la infromación	No se pueden imprimir los documentos físicos y el archivo físico queda retrasado	si	si	si	si	si	si	x			si	si	si	a) Personas: auxiliar contable, contador, gerente financiero, asitente administrativo, director financiero. b) Información y datos: Archivos generados para contorl c) Infraestructura física: Computadores portatiles asistente, contador y financieros d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: Fondos en bancos para pagos h) Socios y proveedores: Clientes y/o
Análisis del impacto del negocio		Demora en la entrega de los productos solicitados al proveedor.	Contar con un listado de proveedores criticos	Esta estretegia nos ayuda a conocer la capacidad de respuesta de los proveedores	Contar con los equipos en los tiempos establecidos	Demora en la entrega de los equipos	si	si	si	si	si	si	x			si	si	si	a) Personas: auxiliar contable, contador, gerente financiero, asitente administrativo, director financiero. b) Información y datos: listado de proveedores criticos c) Infraestructura física: Computadores portatiles asistente, contador y financieros d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet.
Análisis del impacto del negocio	Gestión de Talento	No tener candidatos para la selección de personal requerid	Validadar constantemente el avance de las capacitaciones	Se tiene un archivo donde se almacena toda la informacion en la nube y compartido de las cetificaiones, * Las capacitaciones y/o certificaciones son en linea en	Mantener capacitado al personal	No tener acceso a la información en el momento que se necesite por desconeccion al servidor	si	si	si	si	si	si	x			si	si	si	a) Personas: gerente financiero, asitente administrativo. b) Información y datos: Archivos generados para contorl c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: Fondos en bancos para pagos h) Socios y proveedores: personal activo
Análisis del impacto del negocio		Contratación de personal no competente para el área solicitada.	Selección de personal conforme a competencias establecidas.	Realizar el proceso de contratacion de acuerdo al perfil de puesto.	Desarrollo de actividades de acuerdo al perfil de puesto	Personal seleccionado sin las condiciones requeridas para desarrollar el trabajo a asignar con calidad.	si	si	si	si	si	si	x			si	si	si	a) Personas: Talento Humano b) Información y datos: Procedimiento de Talento Humano c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: personal activo

Análisis del impacto del negocio	Humano	No tener acceso a las capacitaciones	Validadar constantemente el avance de las capacitaciones	Se tiene un archivo donde se almacena toda la informacion en la nube y compartido de las cetificaiones, * Las capacitaciones y/o certificaciones son en linea en	Mantener capacitado al personal	No tener acceso a la información en el momento que se necesite por desconeccion al servidor	si	si	si	si	si	si	X			si	si	si	a) Personas: Talento Humano b) Información y datos: Procedimiento de Talento Humano c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: personal activo
Análisis del impacto del negocio		No tener una retroalimentación de la competencia del personal en los diferentes ámbitos	Realizar evaluación de desempeño laboral.	Evaluaciones de desempeño con criterios de objetividad definidos.	Clima laboral favorable	Al realizar las evaluaciones de desempeño no se cuente con información verdadera	si	si	si	si	si	si	X			si	si	si	a) Personas: Talento Humano b) Información y datos: Procedimiento de Talento Humano c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Proveedores de servicios básicos y tecnológicos
Análisis del impacto del negocio	Marketing e imagen corporativa	Pérdida de credenciales que afectarian la credibilidad con la información pública	Cambio de claves	Realizar el cambio de claves 6 meses	Reduccir el riesgo de pérdidad de información	No realizar el cambio de clave en los tiempos establecidos en la política de seguridad	si	si	si	si	si	si	X			si	si	si	a) Personas: Dirección de Gestión empresarial b) Información y datos: Información de redes sociales c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Proveedores de servicios básicos y tecnológicos
Análisis del impacto del negocio		Pérdida de los archivos	Mantener copias de seguridad	Realizar trimestralmente el respaldo de la información	Contar con los archivos y la información generada para realizar las ppt	No programar el tiempo para realizar el respaldo de la información.	si	si	si	si	si	si	X			si	si	si	a) Personas: Dirección de Gestión empresarial b) Información y datos: Información de redes sociales c) Infraestructura física: Computador d) Equipos y consumibles: N/A e) Sistemas de TIC: Telefonía, correo electronico, internet. f) Transporte y logística: N/A g) Finanzas: N/A h) Socios y proveedores: Proveedores de servicios básicos y tecnológicos

ANEXO 4: PLAN DE CONTINUIDAD DEL NEGOCIO

PLAN DE CONTINUIDAD DEL NEGOCIO DE RADICAL ALTERNATIVAS DE AVANZADA ALTRADICALAVAN CIA. LTDA

CONTENIDO

1. OBJETIVOS

Desarrollar e implementar planes de continuidad a través de actividades y procedimientos que permitan hacer frente a un evento disruptivo, con el objetivo de reanudar y posteriormente restaurar las operaciones.

2. ALCANCE

El presente plan de continuidad del negocio hace referencia al plan de emergencia y contingencia, plan de recuperación, plan de gestión de crisis, plan de comunicaciones, plan de ejercicios y pruebas.

3. MARCO NORMATIVO

- ISO 9001:2015 Sistema de gestión de la calidad. Requisitos.
- ISO 37001:2016 Sistema de gestión antisoborno. Requisitos con orientación para su uso.
- ISO 20000-1:2018 Tecnologías de la información-Gestión del Servicio. Requisitos del sistema de gestión del servicio.
- ISO 27001:2017. Tecnologías de la información — Técnicas de Seguridad — Sistemas de gestión de seguridad de la información
- ISO 22301:2019 Seguridad y resiliencia - Sistemas de gestión de la continuidad del negocio – Requisitos.
- ISO 27701:2019 Técnicas de Seguridad — Extensión a ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la información de privacidad —Requisitos y directrices.

4. RESPONSABILIDADES

- El Gerente General y/o Presidente: Aprobar y hacer cumplir el presente plan.
- El Coordinador del SIG: Revisar el presente plan.
- El Comité de crisis de la empresa: Es responsable de dar estricto cumplimiento al presente plan.

5. DEFINICIONES

- **Plan de emergencia:** Este tipo de planes se encuentran orientados a establecer procedimientos para salvaguardar vidas y evitar posibles lesiones. El objetivo

principal de este tipo de planes es proteger la vida humana contra cualquier amenaza física.

- **Plan de gestión de crisis:** Estos planes cuentan con procedimientos orientados hacer frente a situaciones complejas, que amenacen la reputación y que pongan en riesgo la existencia de una organización.
- **Plan de contingencia:** Planes que cuentan con procedimientos para enfrentar adecuadamente posibles contingencias durante el desarrollo de las actividades para minimizar los impactos en operatividad ante un riesgo.
- **Plan de recuperación:** Planes que cuentan con procedimientos para reanudar las operaciones críticas de una organización a un nivel aceptable por el cliente.
- **Plan de ejercicios y pruebas:** Estos planes establecen procedimientos orientados a probar periódicamente la fortaleza y eficacia del sistema de gestión de continuidad del negocio.
- **Coordinador del plan de continuidad:** Persona nombrada por la dirección de la entidad y está autorizado para desarrollar, implementar, administrar, evaluar, y mantener el programa de continuidad.
- **Comité de continuidad de negocio:** Incluye al coordinador del plan de continuidad y a otras personas que tengan la experiencia, el conocimiento de la entidad y la capacidad para identificar recursos de todas las áreas funcionales claves dentro de la entidad conforme se establece en el documento: **Acta de Junta General Universal Extraordinaria**.
- **MTDP:** Periodo máximo tolerable de disrupción o duración máxima de interrupción aceptable (MAO). Tiempo que tardarían los impactos adversos, que pudieran derivarse de no entregar un producto, prestar un servicio o realizar una actividad, en volverse inaceptables.
- **Plan de continuidad del negocio:** Este tipo de planes consta de información crítica que necesita una empresa para continuar operando durante un evento no planificado.
- **RPO:** Es de Recovery Point Objective - Punto de Recuperación Objetivo ó Pérdida Máxima de Datos (MDL). Punto en el que la información utilizada por una actividad se debe restaurar para permitir la reanudación del funcionamiento de la actividad.
- **RTO:** Iniciales de Recovery Time Objective - Tiempo Objetivo de Recuperación. Tiempo previsto tras un incidente para: la reanudación de la entrega de productos o prestación de servicios, o la reanudación de la actividad, o la recuperación de los recursos.

6. DESARROLLO

El plan de continuidad del negocio incluye estrategias de recuperación para mantener las funciones y procesos críticos o urgentes y suministrar la tecnología de apoyo que respalde estos procesos identificados en la **Matriz de análisis del impacto del negocio (BIA)**

El plan de continuidad es designado para cumplir el RTO (Tiempo objetivo de recuperación) el RPO (Punto objetivo de recuperación); así como también trata las perturbaciones en la cadena de suministros, es actualizado cuatrimestralmente.

El plan de continuidad identifica y documenta lo siguiente:

6.1. Accionistas que necesitan ser notificados

De acuerdo con los planes de continuidad y de ser necesario los accionistas necesitan ser comunicados

6.2. Procesos que deben mantenerse

De acuerdo a la **Matriz de análisis del impacto del negocio (BIA)** los procesos críticos y que deben mantenerse son:

1. Infraestructura.
2. Gestión de TI y Service Desk.
3. Gestión de Continuidad del Negocio.
4. Gestión de compras
5. Gestión de Talento Humano

6.3. Funciones y responsabilidades de los individuos que implementen estrategias de continuidad

Las funciones y responsabilidades de las personas que implementan las estrategias de continuidad se describen en los perfiles de puesto, en los propios planes de continuidad y de carácter general en la siguiente tabla:

Dignidad(cargo)	Función	Responsabilidad	Autoridad
Comité de Continuidad de negocio	Aprobar y evaluar el programa y planes de continuidad.	Asignar los recursos de las áreas funcionales claves dentro de la empresa.	Aprobar los presupuestos necesarios para enfrentar los sucesos. Definir la secuencia de sucesión para continuidad del servicio.
Coordinador del plan de continuidad	Administrar, Implementar y revisar el programa y	Identificar recursos de las áreas funcionales	Tomar decisiones y proveer los recursos asignados necesarios conforme lo establecido en los planes de

	planes de continuidad.	claves dentro de la empresa.	continuidad; y, de ser necesario aprobar el uso de un 10% adicional en los recursos asignados para la entrega a los responsables.
Responsables de los planes de continuidad (Dueños de Proceso)	Ejecutar y mantener el programa y planes de continuidad conforme su responsabilidad	Cumplir con las disposiciones detalladas en los planes de continuidad. Hacer el uso adecuado de los recursos asignados	Activar el plan de continuidad asignado de manera inmediata conforme el suceso. Designar a la persona idónea para continuidad del servicio.

6.4. Procedimiento para activación del plan, incluyendo la autoridad para la activación del plan.

Conforme los sucesos que se presenten, la activación de los planes podría darse en la siguiente estructura.

#	Plan de continuidad	Autoridad para activación del plan	Orden de activación
1	Plan de Emergencia	Jefe de emergencia Comité de continuidad del negocio.	Primera
2	Plan de Continuidad del Negocio	Comité de continuidad del negocio (Gerente General – Director de Operaciones - Coordinador del SIG)	Segunda
3	Plan de contingencia	Director de Operaciones	Tercera
4	Plan de recuperación ante desastres tecnológicos (DRP)	Comité de continuidad del negocio	Cuarta
5	Plan de Gestión de crisis	Comité de crisis	Quinta
6	Procedimiento de comunicación	Comité de Crisis – Gerente de Talento Humano	Sexta

	(Comunicación de crisis)		
7	Plan de Recuperación	Comité de continuidad del negocio-Directores de área – Dueños de procesos	Séptima
8	Programa de ejercicio y pruebas-simulacro	Coordinador del SIG	Permanente

6.5. Tecnología fundamental y susceptible al tiempo, aplicación de sistemas e información.

Dentro de la tecnología con la que cuenta la empresa y es susceptible al tiempo se encuentra:

Equipos críticos

#	Proceso	Equipo	Back up	Descripción
1	Infraestructura	Servidores Físicos y Virtuales Hiperconvergencia Servicio de acceso a Internet	Centro de datos Virtual de Punto Net Equipos de red activa en standby	1 hora
2	Gestión de Ti y Service Desk	Servidor Virtual de Proactivanet Laptops Impresoras	No definido	1 hora
3	Continuidad del Negocio	Comité de Crisis	N/A	N/A
4	Gestión compras	Computador	2	Realizar actividades propias del proceso. Tiempo que puede estar sin la computadora es de máximo 2 horas

5	Gestión Talento Humano	Computador	2	Realizar actividades propias del proceso. Tiempo que puede estar sin la computadora es de máximo 2 horas

Aplicación informática crítico

#	Proceso	Aplicación informática	Descripción
1	Infraestructura	Sistema de Virtualización (Vcenter, Vmware Esxi) Sistema de Respaldos Sistema de Monitoreo Nutanix (Hiperconvergencia)	1 hora
2	Gestión de Ti y Service Desk	Correo electrónico Antivirus Vpn Acronis Servicio de Internet Sistema financiero contable	1 hora
3	Continuidad del Negocio	No Aplica	1 hora
4	Gestión de compras	Office 365	Elaboración de documentación propia del proceso. No puede permanecer sin el programa Office 365
5	Gestión de Talento Humano	Office 365	

Servicios críticos

#	Proceso	Servicio critico	Descripción
1	Infraestructura	Sistema de virtualización Sistema de monitoreo de infraestructura	1 hora
2	Gestión de Ti y Service Desk	Servicio de respaldo de Correo electrónico Mesa de ayuda (Proactivanet)	30 minutos
3	Continuidad del Negocio	Energía eléctrica	Permite el acceso a equipos administrativos. No se puede establecer un tiempo ya que la recuperación del servicio de energía eléctrica debe ser inmediata.
		Internet	Permite el acceso a las aplicaciones on line y nube. No se puede establecer un tiempo ya que la recuperación del servicio de internet debe ser inmediata.
4	Gestión de compras	Energía eléctrica	Permite el acceso a equipos administrativos. No se puede establecer un tiempo ya que la recuperación del servicio de energía eléctrica debe ser inmediata.
		Internet	Permite el acceso a las aplicaciones on line y nube. No se puede establecer un tiempo ya que la recuperación del servicio de internet debe ser inmediata
5	Gestión de Talento Humano	Energía eléctrica	Permite el acceso a equipos administrativos. No se puede establecer un tiempo ya que la recuperación del servicio

			de energía eléctrica debe ser inmediata.
		Internet	Permite el acceso a las aplicaciones on line y nube. No se puede establecer un tiempo ya que la recuperación del servicio de internet debe ser inmediata

Información crítica

#	Proceso	Información critica	Descripción
1	Infraestructura	Respaldos de información generada en los servidores virtuales Registros de los monitoreos	1 hora
2	Gestión de Ti y Service Desk	Registros de atención de tickets de soporte	1 hora
3	Continuidad del Negocio	Plan de continuidad del negocio	Inmediato
4	Gestión de compras	Solicitud y orden de compra	Se ingresa el requerimiento al proveedor seleccionado Tiempo de espera de la cotización 12 horas
		Cotizaciones	Documento donde se determina el valor real de un bien o de un servicio Tiempo de espera de una cotización 24 horas
5	Gestión de Talento Humano	Requerimiento de personal	Documento donde se solicita la contratación de una persona especificando el perfil profesional.

			Tiempo de espera del requerimiento de personal 72 horas
		Hoja de vida	Resumen de estudios, cargos, experiencia laboral que ha desarrollado u obtenido una persona a lo largo de su vida laboral o académica. Tiempo de espera
		Formulario entrevistas	
		Evaluación anual desempeño	Documento para evaluación de capacidades y habilidades. Incumplimiento de requisito.

6.6. Seguridad de información.

Se cuenta con la **Política de seguridad de la información** bajo la responsabilidad del Coordinador del SIG.

En relación con la información la conservación física y digital se describe en la **Elaboración, codificación control documentos registros.**

6.7. Sitios de trabajo alternativo.

Conforme los planes de continuidad, los sitios alternativos de trabajo serán los siguientes:

- Trabajo en casa

6.8. Sitios de trabajo alternativo.

Dentro de los procedimientos alternativos se encuentran:

a) Escenario 1: Suspensión de actividades sin daño o pérdida a los recursos de la empresa.

b) Escenario 2: Suspensión de actividades con daño o pérdida parcial a los recursos de la empresa.
c) Escenario 3: Suspensión de actividades por daño o pérdida total a los recursos de la empresa.
d) Escenario 4: Ausencia de representación judicial y legal en la empresa.
e) Escenario 5: Ausencia de la representación operacional de la gerencia.
f) Escenario 6: Ausencia de liderazgo de operaciones.
g) Escenario 7: Tecnológico
h) Escenario 8: Infraestructura física
i) Escenario 9: Recurso Humano
j) Escenario 9: Proveedores

a. Suspensión de actividades sin daño o pérdida a los recursos de la empresa.

La suspensión de estas actividades podría darse por los siguientes motivos:

1. Geológico (terremoto, erupción volcánica).
2. Meteorológico (inundación, tormenta geomagnética, rayos, granizo, vendavales).
3. Biológico (enfermedades infecciosas, comunicables o pandémicas).
4. Causados accidentalmente por humanos (colapso de estructuras/construcciones, explosión/fuego, recorte de combustible/recursos, derrame o liberación de sustancias peligrosas, falla de equipos, incidente de transporte, indisponibilidad de empleados esenciales, información errada.
5. Causados intencionalmente por humanos (incendios, disturbios civiles, discriminación/ acoso, información errada, actos de guerra, incidentes de seguridad de la información, defectos de productos o contaminación, robo/atraco, huelga nacional, vandalismo).
6. Tecnológico (interrupción, disrupción o falla de conectividad en redes, software o hardware, interrupción, disrupción o falla de herramientas tecnológicas).

b. Suspensión de actividades con daño o pérdida parcial a los recursos de la empresa.

Dependiendo del daño o pérdida del recurso se procederá a su reemplazo inmediato correspondiente. Cuando sea factible.

En el siguiente cuadro se detallan los recursos disponibles como respaldo o Backup.

#	Proceso	Equipo	Back up	Descripción
1	Infraestructura	Servidores Físicos y Virtuales. Hiperconvergencia.	Centro de datos Virtual de Punto Net.	1 hora

		Servicio de acceso a Internet.	Equipos de red activa en standby.	Tiempo en que se puede trabajar sin la utilización del equipo
2	Gestión de Ti y Service Desk	Servidor Virtual de Proactivanet. Laptops. Impresoras.	No definido	1 hora
3	Continuidad del Negocio	Comité de Crisis.		1 hora

Para el caso de que no se cuente con el backup correspondiente el comité de continuidad de negocio gestionará los recursos necesarios con la Gerente General para la asignación correspondiente y restablecer las actividades de forma inmediata.

c. Suspensión de actividades por daño o pérdida total a los recursos de la empresa.

En el caso de presentarse un daño o pérdida total de los recursos de la empresa en el sitio actual del proceso de operaciones, el comité de continuidad de negocio valorará los costos de pérdida versus equipos de backup determinarán la continuidad de operaciones.

Para una referencia del comité de continuidad de negocio en conjunto con la Gerencia General analizará los costos asociados y los tiempos aproximados de adquisición de materiales y equipos para definir si se continúa el negocio.

d. Ausencia de representación judicial y legal en la empresa.

En caso de ausencia de representación judicial y legal de la empresa (fallecimiento o físicamente imposibilitado) se incorporará el representante inmediato según los nombramientos correspondientes. El comité de continuidad del negocio verificará la idoneidad del representante asignado.

Si el representante asignado cumple con el perfil y responsabilidades descrito en el **Perfil de puesto,** será asignado por el período correspondiente.

Si el representante asignado no cumple con el perfil, responsabilidades o presenta algún otro impedimento, se buscará la persona idónea dentro de la misma organización y no ser factible se buscará de afuera. Para esta selección se considerará lo establecido en el **Perfil de puesto,** tomando en cuenta que alguno de estos requisitos establecidos en el perfil de puesto deberá ser cumplidos en un futuro cercano a través del programa de formación.

Para el registro formal se iniciará con el proceso normal de registros en el registro mercantil, superintendencia de compañías, entre otros.

e. Ausencia de la representación operacional de la gerencia.

La ausencia de la Gerencia General en el desarrollo operativo de sus actividades administrativas puede darse por dos casos:

- Ausencia definitiva no prevista. – Se procederá conforme lo establece el punto d; y mientras dure el proceso de nombramiento se asignará una nueva responsable temporal que cumpla con las actividades de Gerencia netamente operacionales (pago de nómina, a proveedores, caja chica).
- Ausencia temporal. – En ausencias planificadas la Gerencia General notificará por los canales de comunicación internos descritos en el **Procedimiento de comunicación**, se proceda conforme se establece en el presente plan, en actividades operacionales de Gerencia.

f. Ausencia de liderazgo de operaciones.

En ausencia del Directo de Operaciones se asignará un responsable temporal que cumpla con las actividades de producción que estuvieron asignadas al director de Operaciones.

En caso de no contar con los responsables asignados en las actividades operativas y administrativas las personas que realicen las actividades temporalmente se considerará conforme se detalla en el **Plan de Contingencia.**

g. Tecnológico.

A continuación, se describe el equipamiento tecnológico, hardware y software, su propósito y ubicación para el restablecimiento de las actividades.

Tipo	Descripción	Propósito

HW & SW	Servidores físicos y virtuales	Esquema de virtualización con sistemas operativos Windows y Linux, que son utilizados para la instalación de los diferentes servicios de la empresa.
SW	Plataforma Gestión de tickets	Gestión de incidencias, peticiones y de niveles de servicio por medio de tickets, todo esto alineado a las buenas prácticas de ITIL.
SW	VPN	Conexiones VPNs en modalidad site to site, mediante las cuales se tiene acceso a las herramientas que van a ser monitoreadas de forma segura.
SW	Correo electrónico	Envío de las notificaciones de alertas de seguridad, posterior al análisis realizado por el personal encargado del monitoreo de las diferentes herramientas.
HW	Estaciones de trabajo	Equipos físicos y/o virtuales que hacen de interfaz entre las herramientas anteriores descritas y el analista.
Servicio	Internet	Permite la comunicación y acceso a los recursos descritos anteriormente.

h. Infraestructura física.

Los sitios alternativos de trabajo serán los siguientes:

#	Proceso	Equipo	Descripción

1	Infraestructura	Servidores Físicos y Virtuales Hiperconvergencia Servicio de acceso a Internet	Centro de datos Virtual Equipos de red activa en standby
		Computadoras & Impresoras	Equipos de computación de oficina

- Instalaciones del cliente.

#	Proceso	Equipo	Descripción	Instalaciones
1	Infraestructura	Servidores Físicos de Hiperconvergencia	Equipos Nutanix	• Contratos con clientes
		Servidores Físicos de Hiperconvergencia	Equipos DELL	• Contratos con clientes
		Servidores Físicos	Equipos HPE	• Contratos con clientes

i. Recurso Humano.

Se ofrece servicios de monitoreo en modalidad 24/7 con analistas (N1 & N2) disponibles en turnos rotativos, por lo tanto, en caso de que algún analista sufra un contratiempo, existen analistas adicionales operando en paralelo para que puedan suplir las actividades y garantizar la continuidad del servicio.

En la tabla siguiente se describe el recurso humano disponible, sus funciones y el equipamiento que maneja.

Actividad principal	Equipamiento
Monitoreo en modalidad 24/7 mediante turnos rotativos y desde las localidades mencionadas en la Tabla 1. Oficinas	Cada analista cuenta con lo siguiente: – Dos computadores (virtual/físico) hardenizados (endurecimiento) – Plan de internet. – Plan de telefonía y datos. – Entorno de pruebas y simulación de modelos.
Analista N1 Monitoreo	Ecuador
Analista N1 Monitoreo	Perú
Analista N1 Monitoreo	Bolivia
Analista N2 SOC	Ecuador
Analista N2 SOC	Perú
Analista N2 SOC	Bolivia
Ser el frente operativo ante los requerimientos del cliente.	Cuenta con lo siguiente: – Dos computadores (virtual/físico) hardenizados (endurecimiento) – Plan de internet. – Plan de telefonía y datos. – Entorno de pruebas y simulación de modelos.
Líder técnico	Ecuador
Gestiona el servicio y la prestación del mismo según los parámetros establecidos a nivel contractual.	Cuenta con lo siguiente: – Dos computadores (virtual/físico) hardenizados (endurecimiento) – Plan de internet. – Plan de telefonía y datos. – Dashboard de control y seguimiento de tickets.
SDM	Ecuador

j. Proveedores.

De acuerdo al contrato, con los proveedores se especifica la fecha de entrega de los equipos por parte del proveedor es de 2 días laborables.

No existen penalidades o indemnizaciones en el caso de no cumplirse en la fecha de la entrega de los equipos.

6.9. Registros vitales

Dentro de los registros vitales se encuentran:

Registros vitales	Responsable	Disponibilidad
Registro revisión de la salud de infraestructura	Responsable del proceso	Digital
Registro de verificación de respaldos y pruebas	Responsable del proceso	Digital
Registro Mantenimientos de Infraestructura de Proyectos	Responsable del proceso	Digital
Mantenimiento de activos de infraestructura	Responsable del proceso	Digital
Matriz registro de mantenimiento y Service Desk	Responsable del proceso	Digital
Mantenimiento de activos de infraestructura	Responsable del proceso	Digital
Plan de Emergencia	Responsable del proceso	Digital
Plan de Continuidad del Negocio	Responsable del proceso	Digital
Matriz de análisis del impacto del negocio (BIA)	Responsable del proceso	Digital
Plan de Contingencia	Responsable del proceso	Digital
Plan de recuperación ante desastres tecnológicos	Responsable del proceso	Digital
Plan de Gestión de Crisis	Responsable del proceso	Digital
Plan de Recuperación	Responsable del proceso	Digital
Solicitud y orden de compra	Responsable del proceso	Digital
Cotizaciones	Proveedor	Física

Orden de compra	Responsable del proceso	Digital

6.10. Lista de contactos

Para el plan de emergencia y planes de continuidad del negocio se cuenta con la lista de contactos evidenciados en el **Plan de evacuación médica.**

6.11. Personal requerido

Cada plan de continuidad establece el personal requerido para el cumplimiento del mismo.

#	Plan	Personal requerido
1	Plan de Emergencia	Brigadas de comunicación, contra incendio, primeros auxilios y evacuación.
2	Plan de continuidad del negocio	Comité de continuidad del negocio. (Coordinador del SIG, Director de Operaciones,
3	Plan de Contingencia	Comité de continuidad del negocio (Presidente, Dueño del proceso de continuidad del negocio, Coordinador de SIG, Dueño del proceso Comercial, Dueños del proceso PostVenta, Oficial de cumplimiento) y Jefe de Brigadas.
4	Plan de recuperación ante desastres tecnológicos	Comité de continuidad del negocio (Presidente, Dueño del proceso de continuidad del negocio, Coordinador de SIG, Dueño del proceso Comercial, Dueños del proceso PostVenta, Oficial de cumplimiento)
5	Plan de gestión de crisis	Comité de continuidad del negocio (Presidente, Dueño del proceso de continuidad del negocio, Coordinador de SIG, Dueño del proceso Comercial, Dueños del proceso PostVenta, Oficial de cumplimiento) , comité de gestión de crisis y Jefe de Brigadas.
6	Procedimiento Comunicación (Comunicación de crisis)	Dueño del proceso Gestión Talento Humano
7	Plan de Recuperación	Comité de continuidad del negocio. (Presidente, Dueño del proceso de continuidad del negocio, Coordinador de SIG, Dueños de procesos, Directores de área, Oficial de cumplimiento)
8	Programa de ejercicio y pruebas	Dueño del proceso de Continuidad del negocio.

6.12. Proveedores que apoyan la continuidad

Los proveedores que apoyan a la continuidad del negocio se detallan en el registro de **Lista de proveedores.**