**PLAN DE TRATAMIENTO DE RIESGOS Y SEGURIDAD DE LA**

**INFORMACIÓN GOBERNACIÓN DEL MAGDALENA**

**Área Funcional de Sistemas**

**Santa Marta D. T. C. e H., enero de 2024**

**OBJETIVOS**

 Desarrollar actividades de modelo de seguridad y Privacidad de la Información permitiendo la integridad, disponibilidad y confidencialidad de los activos de información y comunicación, comprometiendo a todo el talento humano de la Gobernación del Magdalena en los procesos de seguridad, convirtiéndose en una guía que permitirá informar sobre las normas y procedimientos orientados a la seguridad de la información.

 Definir y aplicar las medidas, lineamientos de seguridad en la presente vigencia, como parte del plan de tratamiento para los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en la Gobernación del Magdalena.

 Cumplir con la normatividad Colombiana vigente.

 Propender por la implementación de sistemas de seguridad.

**ALCANCE**

El Plan de Tratamiento de Riesgos y Seguridad de la Información se aplicará a todos los procesos y procedimientos de las diferentes dependencias de la Gobernación del Magdalena, que, para su realización, los servidores públicos se apoyen en tecnologías de la Información o recursos tecnológicos, marcando éste, un derrotero de buenas prácticas que contribuyan a minimizar la contingencia de incidentes que afecten la continuidad y puedan afectar el logro de objetivos de la entidad.

Este plan pretende, demarcar un eficiente tratamiento de riesgos de seguridad digital, integrando los procesos de la entidad, generando buenas prácticas que contribuyan a la toma de decisiones y prevención de incidentes. En éste, se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la entidad.

Este plan incluye guía de controles preventivos y correctivos para incidencias de seguridad de la información, causados por: Ataques maliciosos de origen externo, Ataques maliciosos por origen interno, es decir, causados por malas prácticas de los funcionarios, acceso físico no autorizado a áreas de sistemas a las cuales solo debe ingresar personal del área funcional, administración inadecuada de la red de datos, cambios de datos ocasionados por los servidores públicos que utilizan los Sistemas de Información, los cuales generen pérdida de la integridad de la información, copias de seguridad defectuosas, destrucción de archivos, extracción de información, falsificación de archivos, instalación de software no autorizado, Ilegalidad en Licenciamientos, mal uso de sistemas de información, mal uso de recursos de red, pérdidas de conectividad, pérdida de Contraseñas, pérdida de Código fuente de desarrolladas internamente.

**MARCO NORMATIVO**

 Ley 527 de 1999: Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

 Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

 CONPES 3701 de 2011: Lineamientos de política para ciberseguridad y

Ciberdefensa.

 Ley 1581 de 2012: Por medio de la cual se dictan disposiciones generales para la

Protección de Datos Personales.

 Ley 1221 de 2008: Promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.

 Ley 1712 de 2014: Ley de transparencia y del derecho de acceso a la

Información pública nacional.

 La Ley 1581 de 2012 y decreto 1377 de 2013. Ley de protección de datos personales.

 Ley 1273 de 2009. Ley de delitos informáticos y la protección de la información y de los datos.

 Decreto 1078 de 2015.

 Decreto Único Reglamentario del Sector de Tecnologías de la Información y las

Comunicaciones.

**DEFINICIONES**

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

**Alcance:** Ámbito de la organización que queda sometido al SGSI.

**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

**Análisis de riesgos cualitativo:** Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

**Análisis de riesgos cuantitativo:** Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

**Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

**Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

**Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

**Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza.

**Estimación de riesgos:** Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

**Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.

**Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

**Gestión de activos:** Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos, tratando que cuenten con un nivel adecuado de seguridad.

**Gestión de comunicaciones y operaciones:** Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

**Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje, la información, ya sea impresa, almacenada digitalmente o hablada actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

**Integridad:** Propiedad de la información relativa a su exactitud y completitud.

**Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información, suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.

**Sistema de Gestión de la Seguridad de la Información:** establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

**Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

**Seguridad de los recursos humanos:** Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información, busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

**ETAPAS PARA LA GESTIÓN DEL RIESGO**

De acuerdo con lo señalado en la Guía de Gestión del Riesgo del DAFP, se definen tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la Entidad tener una administración de riesgos acorde con las necesidades de la misma.

1. El Compromiso de la alta y media dirección.

2. Conformación del Comité de Gestión y Desempeño.

3. Capacitación en la metodología.

**TABLA DE VALORACIÓN DE RIESGOS**

Es importante también, determinar y valorar los riesgos de los activos asociados a la información, para así, determinar las acciones a plasmar y emprender en la vigencia del

Plan, a continuación presentamos la Matriz de Riesgos actualizada, para la present e vigencia:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Activo** | **T. De**  **Activo** | **Criticid ad** | **Riesgo** | **Descripci ón Del Riesgo** | **Amenaza** | **Vulnerabilid ades** | **Consecue ncias** | **ANÁLISIS RIESGO INHERENTE** | | |
| **Probabili dad** | **Impacto** | **Zona De**  **Riesgo** |
| Correos Electrón icos Instituci onales | Servici os | BAJO | Pérdi da de la confid encial idad | Filtració n de informa ción instituci onal hacia terceros no autoriza dos | Exposic ión de informa ción instituci onal confide ncial | Despreve nción en la facilitació n de claves de acceso, indebido cierre de cesión, inicio de cesión  permanen te, empleo de IP  inseguras para inicio de cesión | Revelaci  ón de decision es y gestione s institucio nales no validada s, compro miso de informac ión confiden cial, pérdida de la imagen institucio nal,  afectació n emocion al a funciona rios, pérdida de confianz a | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |
| Pérdi da de dispo nibilid ad | Hackeo  de las cuentas de correos electrón icos  que implican restricci ones en el | Jaqueo de las cuentas de correo electrón ico | Despreve  nción en la facilitació n de claves de acceso, indebido cierre de cesión, inicio de cesión | Pérdida  o alteració n de la informac ión histórica que reposa en la cuenta de | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | acceso  y/o bloqueo tempora l |  | permanen  te, empleo de IP  inseguras para inicio de cesión, Ausencia de antivirus, falta de políticas de uso seguro de los equipos  de cómputo, ausencia de restriccion es a descargas de  anuncio emergent es. | correo  electróni co,  envío de correos, autoriza ciones e instrucci ones  con intencion es malignas ajenas a la voluntad institucio nal, investiga ciones penales. |  |  |  |
| Copias de Segurid ad de Informa ción Crítica | Informa ción | Alto | Pérdi da de la confid encial idad | Exposic ión de informa ción  que reposa en las copias de segurid ad | Acceso no autoriza do y modific ación  de informa ción | Indebidos  protocolos de resguardo y protección de la informació n, exposició  n sin restricción de acceso en los dispositiv os de almacena miento de las copias de respaldo, ausencia de | Filtració  n de informac ión institucio nal valiosa y confiden cial, investiga ciones disciplin arias y penales, demand as  contra la entidad, afectació n de la imagen institucio nal, | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | responsa  bles en el custodia de los dispositiv os de almacena miento de las copias de respaldo | pérdida  de informac ión histórica, pérdida de confianz a  ciudada na. |  |  |  |
| Pérdi da de la integri dad | Alteraci ón de la informa ción  que reposa en las copias de segurid ad | Modific ación de la  informa ción | Ausencia de restriccion es de acceso y modificaci ón a la informació n de las copias de respaldo | Inseguri  dad Jurídica e incertidu mbre en la toma de decision es, retrasos en las operacio nes institucio nales,  afectació n del clima laboral, tergivers ación de informac ión, deficent  e defensa judicial, condena s judiciale s,  investiga ciones disciplin arias y penales | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Pérdi da de dispo nibilid ad | Daños en los medios de almace namient o de las copias de segurid ad | Daño tempora l o perman ente del dispositi vo de almace namient o | Indebida  conservac ión y/o falta de mantenimi ento preventivo y correctivo de los dispositiv os de almacena miento de las copias de respaldo, indebido almacena miento | Pérdida de la informac ión, retrasos en las operacio nes institucio nales, pérdida de recursos económi cos, investiga ciones disciplin arias | PROB ABLE | CATA STRÓ FICO | Zona Extrem a |
| Portal Bancari o | Servici os | ALTO | Pérdi da de la confid encial idad | Filtració n de informa ción de claves de acceso o sobre transac ciones | Acceso s no autoriza dos | Fragilidad  en los mecanism os de protección de las claves y usuarios de  acceso, despreve nción en el  suministro de contraseñ as a terceros, ausencia de mecanism os fuertes de seguridad | Acceso no autoriza do al portal, transacci ones perjudici ales, investiga ciones penales, fiscales  y  disciplin arias, pérdida de recursos económi cos | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Pérdi da de dispo nibilid ad | Bloqueo de cuenta de acceso al portal bancari o | Error en la digitació n de usuario  s y claves de acceso | Olvido de claves y usuarios, cambios no autorizad os, indebida digitación, | Restricci  ones de acceso temporal  , afectació n de clima laboral, llamados de atención  , retrasos en operacio nes institucio nales, aplazami ento de las transacci ones. | PROB ABLE | MODE RADO | Zona  Alta |
| Sistemas Transvers ales | Software | Medio | Pérdi da de la confid encial idad | Filtració n de informa ción | Acceso no autoriza do | Deficienci as en la creación de claves de acceso,  vulnerabili dad del sistema de  informació n, ausencia de política de protección de la informació n | Pérdida  de imagen, demand as  contra la entidad, afectació n de clima laboral, afectació n emocion al y de la integrida d del funciona rio, investiga ciones disciplin arias. | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Pérdi da de la integri dad | Alteraci ón de informa ción  que alteren la gestión laboral | Adulter ación de  informa ción | Deficienci as en la asignació n de claves de acceso, vulnerabili dad del sistema  de informació n, ausencia de política de protección de la informació n  sensible. | Pérdida  de imagen, pérdida de la informac ión y/o emplazo de informac ión veraz, incumpli miento de los fines esencial es del Estado,  escalami ento de informac ión ficticia, demand as  contra la entidad, pagos soportad os con informac ión  irreal. | Posible | catastr ófico | Zona Extrem a |
| Pérdi da de dispo nibilid ad | Inutilida d parcial o  tempora l del softwar e | Fallas o inutilida d del servidor o softwar e | Incumplim iento en renovació  n o pagos de licencia o renta del software, falta de  mantenimi ento preventivo o correctivo del servidor o | Restricci ón temporal  de acceso al  software  , retraso en las operacio nes del proceso, pérdida parcial o total de informac | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | equipos  de la red de operación del software | ión,  incumpli miento de metas. |  |  |  |
| Sistema s de informa ción Misional es | Softwar e | ALTO | Pérdi da de la confid encial idad | Filtració n de informa ción sensible | Acceso no autoriza do | Deficienci  as en la asignació n de claves de acceso, vulnerabili dad del sistema  de  informació n, ausencia de política de protección de la informació n  sensible. | Pérdida de imagen, demand as  contra la entidad, afectació n de clima laboral, investiga ciones disciplin arias, daños patrimon iales. | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |
| Pérdi da de la integri dad | Alteraci ón de informa ción. | Adulter ación de  informa ción | Deficienci as en la  asignació n de claves de acceso, vulnerabili dad del  sistema de informació n, ausencia  de política  de protección de la informació n  sensible, ausencia | Pérdida de  imagen, pérdida de la informac ión y/o emplazo  de informac ión  veraz, incumpli  miento  de los fines esencial es del Estado, pérdida de | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | de  mecanism os de verificació n y  control. | recursos  económi cos, escalami ento de informac ión ficticia, demand as  contra la entidad, pagos soportad os con informac ión  irreal, interven ción de organis mos de control |  |  |  |
| Pérdi da de dispo nibilid ad | Inutilida d parcial o  tempora l del Recurs o | Fallas o inutilida d del servidor o softwar e | Incumplim  iento en renovació n o pagos de  licencia o renta del software, falta de mantenimi ento preventivo o correctivo del servidor o equipos  de la red de operación del software | Restricci ón temporal de acceso  al software  , retraso en las operacio nes del proceso, pérdida parcial o total de informac ión. | PROB ABLE | CATA STRÓ FICO | Zona Extrem a |

Grupo de Funcion arios Sistema s de la Gobern ación

Person

as N/A

Pérdi da de dispo nibilid ad

Inopera ncia e incumpli miento en las activida des operativ as: preventi vas y reactiva s del equipo humano de sistema s

Falta de compro miso e ineficien cia

Ausencia de perfiles y/o competen cias técnicas y tecnológic as de acuerdo a las necesidad es de la entidad, falta de compromi so de los servidores

, ausencia de políticas de estímulos e incentivo, ausencia de una política o programa s del área de sistemas, desarticul ación entre los funcionari os y operacion es del

área de sistemas en las diferentes sedes

Inadecu ado o tardío manteni miento de la infraestr uctura

tecnológi ca, operació n

limitada o nula de los

sistemas de informac ión, pérdida de informac ión histórica y de gestión, daños

en las planta tecnológi ca, incumpli miento

de entrega de reportes, informes

, incumpli miento de

metas

CASI SEGU RO

CATA STRÓ FICO

Zona Extrem a

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Red de ordenad ores | Compo nentes de red | BAJO | Pérdi da de dispo nibilid ad | Inutilida d parcial o total de la red de  ordenad ores | Daños en la red | Falta de  mantenimi ento preventivo y correctivo de la red de ordenador es, falta  de mantenimi ento a la infraestru ctura  física o eléctrica, limitada inversión a las  necesidad es de mejoras de la red | Inoperan cia de la red, dificultad es de acceso a la conectivi dad de internet, program as o comparti miento  de archivos, retrasos en las operacio nes laborale s. | PROB ABLE | CATA STRÓ FICO | Zona Extrem a |
| Equipos tecnoló gicos (scanne r, impreso ras, video beam, Router, accesori os) | Hardw are | BAJO | Pérdi da de dispo nibilid ad | Inutilida d de los equipos tecnoló gicos | Daños en los equipos tecnoló gicos | Falta de  mantenimi ento preventivo y correctivo de los equipos tecnológic os, falta  de mantenimi ento a la infraestru ctura  física o eléctrica, limitada inversión a las  necesidad es de mejoras de la infraestru ctura | Pérdida  de recursos económi cos, limitacio nes en las operacio nes,  cese temporal de algunas actividad es, insatisfa cción de clientes internos  y externos  ,  incumpli miento de | PROB ABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | tecnológic  a | metas,  no entrega de reportes o informes |  |  |  |
| Aplicativ os Web nacional es administ rado por las diversas secretar ias o áreas (SISPR O, ADRES, SUPER SALUD  , SEPPI, SIMIT, ETC) | Servici os | BAJO | Pérdi da de dispo nibilid ad | Bloqueo de cuenta de acceso a los  portales o aplicativ os web | Error en la digitació n de usuario  s y claves de acceso | Olvido de claves y usuarios, cambios no autorizad os, indebida digitación, | Restricci  ones de acceso temporal  , afectació n de clima laboral, llamados de atención  ,  retrasos en operacio nes institucio nales, sancione s por reportes extempo ráneos, pérdida de imagen, afectació n de indicado res. | IMPRO BABLE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Internet Corpora tivo | Servici os | BAJO | Pérdi da de dispo nibilid ad | Interrup ción de la conexió n a internet | Daños o inopera ncia en la conexió n | Daños en la infraestru ctura tecnológic a, pago inoportun o en el servicio  de internet, ausencia de acciones de mantenimi ento preventivo y correctivo de la red cableada, punto de red o los shwiches. | Interrupc  ión de la conectivi dad, interrupc ión de trámites, servicios y operacio nes soportad as en internet, insatisfa cción de la comunid ad, retraso en las operacio nes, incumpli miento de  metas y objetivos institucio nales | IMPRO BABLE | MODE RADO | Zona Moder ada |
| Sistema operativ os y herrami entas ofimátic as | Softwar e | BAJO | Pérdi da de la integri dad | Afectaci ón con virus del  sistema operativ o, pogram as o herrami entas ofimátic as licencia das | Infecció n de progra mas o sistema s | Expiració  n del porgrama antivirus, uso de licencias free, error en la digitación de licencias, no verificació n de las condicion es de desinfecci ón de dispositiv os de | Inoperan cia temporal de los equipos de cómputo  , retrasos en operacio nes laborale s | PROB ABLE | MAYO R | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | almacena  miento  USB. |  |  |  |  |
| Pérdi da de dispo nibilid ad | Inutilida d parcial o total de los  equipos de cómput o por daño en el sistema operativ o o herrami entas ofimátic as | Daños en sistema operativ o oprogra mas | Expiració  n del porgrama antivirus, uso de licencias free, error en la digitación de licencias, no verificació n de las condicion es de desinfecci ón de dispositiv os de almacena miento USB, mal uso de los equipos, indebido procedimi ento de apagado  o reinicio. | Limitacio  nes en las operacio nes,  cese temporal de algunas actividad es, pérdida de informac ión, insatisfa cción de clientes internos  y externos  , no entrega de reportes e informes  , sancione s | PROB ABLE | MAYO R | Zona Extrem a |
| Bases de Datos de las depend encias | Informa ción | ALTO | Pérdi da de la confid encial idad | Exposic ión de informa ción  que reposa en las Bases de Datos  corporat ivas | Acceso no autoriza do | Indebidos  protocolos de resguardo y protección de los equipos que poseen  las base de datos, exposició | Filtració  n de informac ión institucio nal valiosa y confiden cial, investiga ciones disciplin arias y | POSIB LE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | n sin  restricción de acceso en los dispositiv os de almacena miento de las bases de datos. | penales,  demand as  contra la entidad, afectació n de la imagen institucio nal, pérdida de informac ión histórica, pérdida de confianz a  ciudada na. |  |  |  |
| Pérdi da de la integri dad | Alteraci ón de la informa ción  que reposa en las bases de datos | Modific ación de la  informa ción | Ausencia de restriccion es de acceso y modificaci ón a la informació n de las bases de datos | Inseguri  dad Jurídica e incertidu mbre en la toma de decision es, retrasos en las operacio nes institucio nales,  afectació n del clima laboral, investiga ciones disciplin arias y penales | POSIB LE | CATA STRÓ FICO | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Pérdi da de dispo nibilid ad | Daños en los medios de almace namient o de las bases de  datos | Daño tempora l o perman ente del equipo donde reposa  la base de datos | Indebida conservac ión y/o falta de mantenimi ento preventivo y correctivo de los equipos  de cómputo que contienen las bases de datos | Pérdida  de la informac ión, retrasos en las operacio nes institucio nales, pérdida de recursos económi cos, investiga ciones disciplin arias, no entrega de reportes e informes  , desconfi anza ciudada na | PROB ABLE | CATA STRÓ FICO | Zona Extrem a |
| Sistema de Cortafu egos | Softwar e | BAJO | Pérdi da de la confid encial idad | Filtració n hacia informa ción sensible de la entidad | Acceso no autoriza do | Ausencia de un sistema de  bloqueo el acceso no autorizad  o a la red privada de la entidad, ataques  cibernétic os. | Filtració  n de informac ión institucio nal valiosa y confiden cial, investiga ciones disciplin arias y penales, demand as  contra la entidad, afectació n de la imagen | CASI SEGU RO | MAYO R | Zona Extrem a |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | institucio  nal, pérdida de informac ión. |  |  |  |
| Sistema de antivirus | Softwar e | BAJO | Pérdi da de dispo nibilid ad | Afectaci ón con virus del  sistema operativ o, pogram as o utilidad es. | Infecció n de progra mas o sistema s | Expiració  n del porgrama antivirus, no verificació n de las condicion es de desinfecci ón de dispositiv os de almacena miento USB, ausencia de restriccion es de visitas a sitios potencial mente peligrosos  , ausencia  de bloqueo de  elementos emergent es. | Limitacio nes en las operacio nes,  cese temporal de algunas actividad es, pérdida de informac ión, insatisfa cción de clientes internos  y externos  . | CASI SEGU RO | CATA STRÓ FICO | Zona Extrem a |

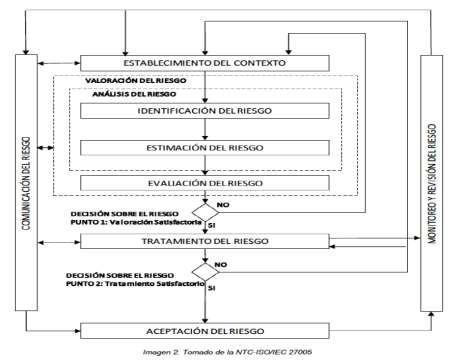
**VISION GENERAL PARA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN**

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

 Proceso para la Administración del Riesgo:



 Proceso para la Administración del riesgo en Seguridad de la Información:



**PLAN DE ACTIVIDADES POR RIESGO DETERMINADO**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Activo** | **T. de Activo** | **Riesgo** | **Amenaza** | **Actividad** | **Fecha de**  **Inicio** | **Fecha de**  **Terminación** | **Periodicidad** |
| Correos Electrónicos Institucional es | Servicios | Pérdida de la confidencialidad | Exposición de información institucional confidencial | sensibilización | febrero de  2024 | Diciembre de  2024 | Semestral |
| Pérdida de disponibilidad | Hackeo de las cuentas de correo electrónico |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Copias de Seguridad de Información Crítica | Información | Pérdida de la confidencialidad | Acceso no autorizado y modificación de información | 1. Generación de Backup.  2. Adquisición de herramientas para la custodia de las copias de Seguridad. | Enero de  2024 | Diciembre de  2024 | Semanal |
| Pérdida de la integridad | Modificación de la información |
| Pérdida de disponibilidad | Daño temporal o permanente del dispositivo de almacenamient o |
| Portal  Bancario | Servicios | Pérdida de la confidencialidad | Accesos no autorizados | Sensibilización a las áreas encargadas del uso de éstos | mayo de  2024 | Diciembre de  2024 | Semestral |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Pérdida de disponibilidad | Error en la digitación de usuarios y claves de acceso |  |  |  |  |
| Sistemas Transversal es | Software | Pérdida de la confidencialidad | Acceso no autorizado | Verificación y Monitoreo de buen uso por parte de funcionarios / Generación de Roles / Sensibilización de Manejo de Password | Abril de  2024 | Diciembre de  2024 | Trimestral |
| Pérdida de la integridad | Adulteración de información |
| Pérdida de disponibilidad | Fallas o inutilidad del servidor o software |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sistemas de información Misionales | Software | Pérdida de la confidencialidad | Acceso no autorizado | Verificación y Monitoreo de buen uso por parte de funcionarios / Generación de Roles / Sensibilización de Manejo de Password | Marzo de  2024 | Diciembre de  2024 | Semanal |
| Pérdida de la integridad | Adulteración de información |
| Pérdida de disponibilidad | Fallas o inutilidad del servidor o software | Mantener Sistemas  Alternativos de Respaldo |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Red de ordenadores | Component es de red | Pérdida de disponibilidad | Daños en la red | Mantener Monitoreo de  Red. | Enero de  2024 | Diciembre de  2024 | Trimestralment e |
| Equipos tecnológicos (scanner, impresoras, video bean, Reuters, accesorios) | Hardware | Pérdida de disponibilidad | Daños en los equipos tecnológicos | Diseñar plan de mejoramiento de alimentación eléctrica y verificar condiciones físicas de áreas, para el correcto funcionamiento de los equipos | junio de  2024 | Diciembre de  2024 |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Aplicativos  Web nacionales administrado por las diversas secretarias o áreas (SISPRO, ADRES, SUPERSAL UD , SEPPI, SIMIT, ETC) | Servicios | Pérdida de disponibilidad | Error en la digitación de usuarios y claves de acceso | Sensibilización para el manejo de Password | Abril de  2024 | Diciembre de  2024 | Semestral |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sistema operativos y herramienta s ofimáticas | Software | Pérdida de la integridad | Infección de programas o sistemas | Gestión de Niveles de seguridad con antivirus | enero de  2024 | Diciembre de  2024 |  |
| Pérdida de disponibilidad | Daños en sistema operativo o programas |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sistema de  Cortafuegos | Software | Pérdida de la confidencialidad | Acceso no autorizado | Implementación de nuevas políticas en el  Firewall / monitoreo / Adquisición de firewall para la Sec Salud | Enero de  2024 | Diciembre de  2024 | Semestral |
| Sistema de antivirus | Software | Pérdida de disponibilidad | Infección de programas o sistemas | Renovación de Licencias  Antivirus | Febrero de 2024 | Diciembre de  2024 |  |