



GOBERNACIÓN DEL
MAGDALENA



La fuerza
del cambio



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 2023





OBJETIVOS

- Definir un nuevo 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 presente vigencia:

Activo	T. De Activo	Críticidad	Riesgo	Descripción Del Riesgo	Amenaza	Vulnerabilidades	Consecuencias	ANÁLISIS RIESGO INHERENTE		
								Probabilidad	Impacto	Zona De Riesgo
Correos Electrónicos Institucionales	Servicios	BAJO	Pérdida de la confidencialidad	Filtración de información institucional hacia terceros no autorizados	Exposición de información institucional confidencial	Desprevección en la facilitación de claves de acceso, indebido cierre de cesión, inicio de cesión permanente, empleo de IP inseguras para inicio de cesión	Revelación de decisiones y gestiones institucionales no validadas, compromiso de información confidencial, pérdida de la imagen institucional, afectación emocional a funcionarios, pérdida de confianza	IMPROBABLE	CATASTRÓFICO	Zona Extrema
			Pérdida de disponibilidad	Hackeo de las cuentas de correos electrónicos que implican restricciones en el	Jaqueo de las cuentas de correo electrónico	Desprevección en la facilitación de claves de acceso, indebido cierre de cesión, inicio de cesión	Pérdida o alteración de la información histórica que reposa en la cuenta de			





				acceso y/o bloqueo temporal		permanente, empleo de IP inseguras para inicio de cesión, Ausencia de antivirus, falta de políticas de uso seguro de los equipos de cómputo, ausencia de restricciones a descargas de anuncio emergentes.	correo electrónico, envío de correos, autorizaciones e instrucciones con intenciones malignas ajenas a la voluntad institucional, investigaciones penales.			
Copias de Seguridad de Información Crítica	Información	Alto	Pérdida de la confidencialidad	Exposición de información que reposa en las copias de seguridad	Acceso no autorizado y modificación de información	Indebidos protocolos de resguardo y protección de la información, exposición sin restricción de acceso en los dispositivos de almacenamiento de las copias de respaldo, ausencia de	Filtración de información institucional valiosa y confidencial, investigaciones disciplinarias y penales, demandas contra la entidad, afectación de la imagen institucional,	IMPROBABLE	CATASTRÓFICO	Zona Extrema





MAGDALENA

La fuerza del cambio



					responsables en el custodia de los dispositivos de almacenamiento de las copias de respaldo	pérdida de información histórica, pérdida de confianza ciudadana.				
			Pérdida de la integridad	Alteración de la información que reposa en las copias de seguridad	Modificación de la información	Ausencia de restricciones de acceso y modificación a la información de las copias de respaldo	Inseguridad Jurídica e incertidumbre en la toma de decisiones, retrasos en las operaciones institucionales, afectación del clima laboral, tergiversación de información, deficiente defensa judicial, condenas judiciales, investigaciones disciplinarias y penales	IMPROBABLE	CATASTRÓFICO	Zona Extrema





			Pérdida de disponibilidad	Daños en los medios de almacenamiento o de las copias de seguridad	Daño temporal o permanente del dispositivo de almacenamiento	Indebida conservación y/o falta de mantenimiento preventivo y correctivo de los dispositivos de almacenamiento de las copias de respaldo, indebido almacenamiento	Pérdida de la información, retrasos en las operaciones institucionales, pérdida de recursos económicos, investigaciones disciplinarias	PROBABLE	CATASTRÓFICO	Zona Extrema
Portal Bancario	Servicios	ALTO	Pérdida de la confidencialidad	Filtración de información de claves de acceso o sobre transacciones	Accesos no autorizados	Fragilidad en los mecanismos de protección de las claves y usuarios de acceso, desprevisión en el suministro de contraseñas a terceros, ausencia de mecanismos fuertes de seguridad	Acceso no autorizado al portal, transacciones perjudiciales, investigaciones penales, fiscales y disciplinarias, pérdida de recursos económicos	IMPROBABLE	CATASTRÓFICO	Zona Extrema





			Pérdida de disponibilidad	Bloqueo de cuenta de acceso al portal bancario	Error en la digitación de usuarios y claves de acceso	Olvido de claves y usuarios, cambios no autorizados, indebida digitación,	Restricciones de acceso temporal, afectación de clima laboral, llamados de atención, retrasos en operaciones institucionales, aplazamiento de las transacciones.	PROBABLE	MODERADO	Zona Alta
Sistemas Transversales	Software	Medio	Pérdida de la confidencialidad	Filtración de información	Acceso no autorizado	Deficiencias en la creación de claves de acceso, vulnerabilidad del sistema de información, ausencia de política de protección de la información	Pérdida de imagen, demandas contra la entidad, afectación de clima laboral, afectación emocional y de la integridad del funcionario, investigaciones disciplinarias.	IMPROBABLE	CATASTRÓFICO	Zona Extrema





			Pérdida de la integridad	Alteración de información que alteren la gestión laboral	Adulteración de información	Deficiencias en la asignación de claves de acceso, vulnerabilidad del sistema de información, ausencia de política de protección de la información sensible.	Pérdida de imagen, pérdida de la información y/o emplazo de información veraz, incumplimiento de los fines esenciales del Estado, escalamiento de información ficticia, demandas contra la entidad, pagos soportados con información irreal.	Possible	catastrófico	Zona Extrema
			Pérdida de disponibilidad	Inutilidad parcial o temporal del software	Fallas o inutilidad del servidor o software	Incumplimiento en renovación o pagos de licencia o renta del software, falta de mantenimiento preventivo o correctivo del servidor o	Restricción temporal de acceso al software, retraso en las operaciones del proceso, pérdida parcial o total de informac	IMPROBABLE	CATASTRÓFICO	Zona Extrema





						equipos de la red de operación del software	ión, incumplimiento de metas.			
Sistemas de información Misionales	Software	ALTO	Pérdida de la confidencialidad	Filtración de información sensible	Acceso no autorizado	Deficiencias en la asignación de claves de acceso, vulnerabilidad del sistema de información, ausencia de política de protección de la información sensible.	Pérdida de imagen, demandas contra la entidad, afectación de clima laboral, investigaciones disciplinarias, daños patrimoniales.	IMPROBABLE	CATASTRÓFICO	Zona Extrema
			Pérdida de la integridad	Alteración de información.	Adulteración de información	Deficiencias en la asignación de claves de acceso, vulnerabilidad del sistema de información, ausencia de política de protección de la información sensible, ausencia	Pérdida de imagen, pérdida de la información y/o emplazo de información veraz, incumplimiento de los fines esenciales del Estado, pérdida de	IMPROBABLE	CATASTRÓFICO	Zona Extrema





					de mecanismos de verificación y control.	recursos económicos, escalamiento de información ficticia, demandas contra la entidad, pagos soportados con información irreal, intervención de organismos de control			
		Pérdida de disponibilidad	Inutilidad parcial o temporal del Recurso	Fallas o inutilidad del servidor o software	Incumplimiento en renovación o pagos de licencia o renta del software, falta de mantenimiento preventivo o correctivo del servidor o equipos de la red de operación del software	Restricción temporal de acceso al software, retraso en las operaciones del proceso, pérdida parcial o total de información.	PROBABLE	CATASTRÓFICO	Zona Extrema





Grupo de Funcionarios Sistemas de la Gobernación	Personas	N/A	Pérdida de disponibilidad	Inoperancia e incumplimiento en las actividades operativas: preventivas y reactivas del equipo humano de sistemas	Falta de compromiso e ineficiencia	Ausencia de perfiles y/o competencias técnicas y tecnológicas de acuerdo a las necesidades de la entidad, falta de compromiso de los servidores, ausencia de políticas de estímulos e incentivo, ausencia de una política o programas del área de sistemas, desarticulación entre los funcionarios y operaciones del área de sistemas en las diferentes sedes	Inadecuado o tardío mantenimiento de la infraestructura tecnológica, operación limitada o nula de los sistemas de información, pérdida de información histórica y de gestión, daños en las planta tecnológica, incumplimiento de entrega de reportes, informes, incumplimiento de metas	CASI SEGURO	CATASTRÓFICO	Zona Extrema
--	----------	-----	---------------------------	---	------------------------------------	---	---	-------------	--------------	--------------





Red de ordenadores	Componentes de red	BAJO	Pérdida de disponibilidad	Inutilidad parcial o total de la red de ordenadores	Daños en la red	Falta de mantenimiento preventivo y correctivo de la red de ordenadores, falta de mantenimiento a la infraestructura física o eléctrica, limitada inversión a las necesidades de mejoras de la red	Inoperancia de la red, dificultades de acceso a la conectividad de internet, programas o compartimiento de archivos, retrasos en las operaciones laborales.	PROBABLE	CATASTRÓFICO	Zona Extrema
Equipos tecnológicos (scanner, impresoras, video beam, Router, accesorios)	Hardware	BAJO	Pérdida de disponibilidad	Inutilidad de los equipos tecnológicos	Daños en los equipos tecnológicos	Falta de mantenimiento preventivo y correctivo de los equipos tecnológicos, falta de mantenimiento a la infraestructura física o eléctrica, limitada inversión a las necesidades de mejoras de la infraestructura	Pérdida de recursos económicos, limitaciones en las operaciones, cese temporal de algunas actividades, insatisfacción de clientes internos y externos, incumplimiento de	PROBABLE	CATASTRÓFICO	Zona Extrema





						tecnológica	metas, no entrega de reportes o informes			
Aplicativos Web nacional es administrado por las diversas secretarías o áreas (SISPRO, ADRES, SUPER SALUD, SEPP, SIMIT, ETC)	Servicios	BAJO	Pérdida de disponibilidad	Bloqueo de cuenta de acceso a los portales o aplicativos web	Error en la digitación de usuarios y claves de acceso	Olvido de claves y usuarios, cambios no autorizados, indebida digitación,	Restricciones de acceso temporal, afectación de clima laboral, llamados de atención, retrasos en operaciones institucionales, sanciones por reportes extemporáneos, pérdida de imagen, afectación de indicadores.	IMPROBABLE	CATASTRÓFICO	Zona Extrema





Internet Corporativo	Servicios	BAJO	Pérdida de disponibilidad	Interrupción de la conexión a internet	Daños o inoperancia en la conexión	Daños en la infraestructura tecnológica, pago inoportuno en el servicio de internet, ausencia de acciones de mantenimiento preventivo y correctivo de la red cableada, punto de red o los switches.	Interrupción de la conectividad, interrupción de trámites, servicios y operaciones soportadas en internet, insatisfacción de la comunidad, retraso en las operaciones, incumplimiento de metas y objetivos institucionales	IMPROBABLE	MODERADO	Zona Moderada
Sistema operativos y herramientas ofimáticas	Software	BAJO	Pérdida de la integridad	Afectación con virus del sistema operativo, programas o herramientas ofimáticas licencias	Infección de programas o sistemas	Expiración del programa antivirus, uso de licencias free, error en la digitación de licencias, no verificación de las condiciones de desinfección de dispositivos de	Inoperancia temporal de los equipos de cómputo, retrasos en operaciones laborales	PROBABLE	MAYOR	Zona Extrema





						almacena miento USB.				
			Pérdida de disponibilidad	Inutilidad parcial o total de los equipos de cómputo por daño en el sistema operativo o herramientas ofimáticas	Daños en sistema operativo o programas	Expiración del programa antivirus, uso de licencias free, error en la digitación de licencias, no verificación de las condiciones de desinfección de dispositivos de almacenamiento USB, mal uso de los equipos, indebido procedimiento de apagado o reinicio.	Limitaciones en las operaciones, cese temporal de algunas actividades, pérdida de información, insatisfacción de clientes internos y externos, no entrega de reportes e informes, sanciones	PROBABLE	MAYOR	Zona Extrema
Bases de Datos de las dependencias	Información	ALTO	Pérdida de la confidencialidad	Exposición de información que reposa en las Bases de Datos corporativas	Acceso no autorizado	Indebidos protocolos de resguardo y protección de los equipos que poseen las bases de datos, exposición	Filtración de información institucional valiosa y confidencial, investigaciones disciplinarias y	POSIBLE	CATASTRÓFICO	Zona Extrema





MAGDALENA

La fuerza del cambio



					n sin restricción de acceso en los dispositivos de almacenamiento de las bases de datos.	penales, demandas contra la entidad, afectación de la imagen institucional, pérdida de información histórica, pérdida de confianza ciudadana.				
			Pérdida de la integridad	Alteración de la información que reposa en las bases de datos	Modificación de la información	Ausencia de restricciones de acceso y modificación a la información de las bases de datos	Inseguridad Jurídica e incertidumbre en la toma de decisiones, retrasos en las operaciones institucionales, afectación del clima laboral, investigaciones disciplinarias y penales	POSIBLE	CATASTRÓFICO	Zona Extrema





			Pérdida de disponibilidad	Daños en los medios de almacenamiento de las bases de datos	Daño temporal o permanente del equipo donde reposa la base de datos	Indebida conservación y/o falta de mantenimiento preventivo y correctivo de los equipos de cómputo que contienen las bases de datos	Pérdida de la información, retrasos en las operaciones institucionales, pérdida de recursos económicos, investigaciones disciplinarias, no entrega de reportes e informes, desconfianza ciudadana	PROBABLE	CATASTRÓFICO	Zona Extrema
Sistema de Cortafuegos	Software	BAJO	Pérdida de la confidencialidad	Filtración hacia información sensible de la entidad	Acceso no autorizado	Ausencia de un sistema de bloqueo el acceso no autorizado a la red privada de la entidad, ataques cibernéticos.	Filtración de información institucional valiosa y confidencial, investigaciones disciplinarias y penales, demandas contra la entidad, afectación de la imagen	CASI SEGURO	MAYOR	Zona Extrema





							institucional, pérdida de información.			
Sistema de antivirus	Software	BAJO	Pérdida de disponibilidad	Afectación con virus del sistema operativo, programas o utilidades.	Infección de programas o sistemas	Expiración del programa antivirus, no verificación de las condiciones de desinfección de dispositivos de almacenamiento USB, ausencia de restricciones de visitas a sitios potencialmente peligrosos, ausencia de bloqueo de elementos emergentes.	Limitaciones en las operaciones, cese temporal de algunas actividades, pérdida de información, insatisfacción de clientes internos y externos.	CASI SEGURO	CATASTRÓFICO	Zona Extrema

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:

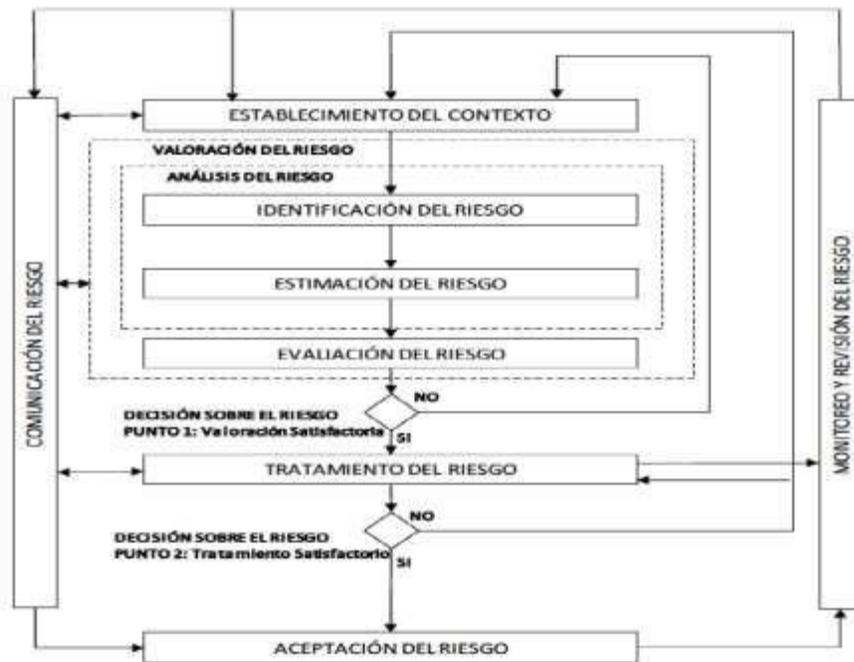


Imagen 2. Tomado de la NTC-ISO/IEC 27005





PLAN DE ACTIVIDADES POR RIESGO DETERMINADO

Activo	T. de Activo	Riesgo	Amenaza	Actividad	Fecha de Inicio	Fecha de Terminación	Periodicidad
Correos Electrónicos Institucionales	Servicios	Pérdida de la confidencialidad	Exposición de información institucional confidencial	sensibilización	febrero de 2023	Diciembre de 2023	Semestral
		Pérdida de disponibilidad	Jaqueo 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 2023	Diciembre de 2023	Semanal
		Pérdida de la integridad	Modificación de la información				
		Pérdida de disponibilidad	Daño temporal o permanente del dispositivo de almacenamiento				
Portal Bancario	Servicios	Pérdida de la confidencialidad	Accesos no autorizados	Sensibilización a las áreas encargadas del uso de éstos	mayo de 2023	Diciembre de 2023	Semestral



		Pérdida de disponibilidad	Error en la digitación de usuarios y claves de acceso				
Sistemas Transversales	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 2023	Diciembre de 2023	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 2023	Diciembre de 2023	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	Componentes de red	Pérdida de disponibilidad	Daños en la red	Mantener Monitoreo de Red.	Enero de 2023	Diciembre de 2023	Trimestralmente
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 2023	Diciembre de 2023	



Aplicativos Web nacionales administrado por las diversas secretarías o áreas (SISPRO, ADRES, SUPERSALUD, 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 2023	Diciembre de 2023	Semestral
---	-----------	---------------------------	---	--	---------------	-------------------	-----------



Sistema operativos y herramientas ofimáticas	Software	Pérdida de la integridad	Infección de programas o sistemas	Gestión de Niveles de seguridad con antivirus	enero de 2023	Diciembre de 2023	
		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 2023	Diciembre de 2023	Semestral
Sistema de antivirus	Software	Pérdida de disponibilidad	Infección de programas o sistemas	Renovación de Licencias Antivirus	Febrero de 2023	Diciembre de 2023	