GOBERNACIÓN de BOLÍVAR

Plan General para el Tratamiento de Riesgos de Seguridad de la Información.

Gobernación de Bolívar
Dirección de Tecnologías de la Información y las Comunicaciones

FIRMAS Y REVISIONES

TITULO	Plan General para el Tratamiento de Riesgos de Seguridad de la Información.
Autor	Dirección de las Tecnologías de la Información y las Comunicaciones - Gobernación de Bolívar
Tema	Política de Tecnología de Información y Comunicación, Estrategia Gobierno Digital
Fecha de Elaboración	Diciembre 2018
Formato	PDF
Versión	1.0
Palabras Relacionadas	Modelo de Gestión TI, Tecnología de Información – TI, Gobierno Digital

CONTROL DE CAMBIOS

Fecha	Autor	Versión	Cambio
28 de diciembre 2018	Dirección TIC	1.0	Versión Inicial
26 de diciembre 2019	Dirección TIC	2.0	Se detalló la evaluación del riesgo asociados la seguridad y privacidad de la información
30 de noviembre 2020	Dirección TIC	3.0	Se definieron de manera general los riesgos, vulnerabilidades y amenazas. Se incluyeron los controles según la norma ISO/IEC 27002:2013

TABLA DE CONTENIDO

INTRODUCCIÓN

La revolución digital está obligando a reconocer el protagonismo de la información en los procesos productivos de todas las empresas y la importancia de tenerla adecuadamente identificada y protegida. Por lo anterior, se amerita dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La GOBERNACIÓN DE BOLÍVAR, atendiendo a su política general de seguridad y privacidad de la información, previamente aprobada, ha decidido vincular un modelo de administración de los riesgos de seguridad de la información el logro de los objetivos de mantener la información de la Entidad confidencial, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de la información se enmarcan en:

- **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2. OBJETIVO

Establecer en la GOBERNACIÓN DE BOLIVAR una ruta con enfoque metódico que facilite las pautas necesarias para desarrollar y fortalecer una correcta gestión de los riesgos de seguridad de la información, a través de metodologías que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y la generación de políticas.

3. ALCANCE

La gestión de riesgos será aplicada sobre cualquier proceso de la GOBERNACIÓN DE BOLÍVAR, a través de los principios básicos para la administración de los riesgos de seguridad de la información. Dicha gestión, incluye las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

4. TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información:

✓ **Administración del riesgo:** conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

✓ **Activo de Información**: en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

✓ **Análisis de riesgos**: es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

✓ **Amenaza:** es la causa potencial de una situación de incidente y no deseada por la organización

✓ **Causas**: son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

✓ **Consecuencia**: resultado de un evento que afecta los objetivos.

✓ **Criterios del riesgo**: términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

✓ **Control**: medida que modifica el riesgo.

✓ **Evaluación de riesgos**: proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

✓ **Evento**: un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

✓ **Estimación del riesgo:** proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

✓ **Evitación del riesgo:** decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

✓ **Factores de riesgo:** situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

✓ **Gestión del riesgo**: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

✓ **Identificación del riesgo.:** proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

✓ **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.

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

✓ **Impacto: c**ambio adverso en el nivel de los objetivos del negocio logrados.

✓ **Nivel de riesgo**: magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

✓ **Matriz de riesgos:** instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

✓ **Monitoreo**: mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

✓ **Propietario del riesgo**: persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

✓ **Proceso**: conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

✓ **Riesgo inherente**: es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

✓ **Riesgo Residual**: el riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

✓ **Riesgo**: efecto de la incertidumbre sobre los objetivos.

✓ **Riesgo en la seguridad de la información:** potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

✓ **Reducción del riesgo:** acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

✓ **Retención del riesgo:** aceptación de la pérdida o ganancia proveniente de un riesgo particular

✓ **Seguimiento**: mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

✓ **Tratamiento del riesgo**: proceso para modificar el riesgo (Icontec Internacional, 2011).

✓ **Valoración del riesgo**: proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

✓ **Vulnerabilidad:** es aquella debilidad de un activo o grupo de activos de información

✓ **Seguridad de la información**: preservación de la confidencialidad, integridad y disponibilidad de la información.

✓ **SGSI**: Sistema de Gestión de Seguridad de la Información.

5. RIESGO = (AMENAZA*VULNERABILIDAD).

TIPO DE ACTIVO DE INFORMACIÓN	DATOS																			
AMENAZA	Código malicioso					Divulgación no autorizada de información sensible o crítica					Error operacional del personal		Robo o pérdida de información sensible o crítica					Modificación No autorizada de Información		
VULNERABILIDAD	Falta /falla de gestión de medios removibles	Falta/ falla de gestión de acceso de usuarios	Falta/Falla de gestión de herramientas para detección y prevención de código malicioso	Falta/falla de gestión sobre la infraestructura de red	Falta de concientización de los usuarios	Falta de mecanismos de cifrado de datos	Eliminación de datos de forma no segura o Inadecuada	Falta/ falla de gestión de acceso de usuarios	Falta de acuerdos de confidencialidad	Falta / Deficiencia en el procedimiento de identificación , clasificación y manejo de la información	Falta / Deficiencia en el procedimiento de identificación , clasificación y manejo de la información	Falta de capacitación de los usuarios	Falta de mecanismos de cifrado de datos	Falta/ falla de gestión de acceso de usuarios	Falta de seguridad en el intercambio de información	Falta / Deficiencia en el procedimiento de identificación , clasificación y manejo de la información	Falta de concientización de los usuarios	Falta/Falla en la gestión de herramientas y logs de auditoria	Falta de seguridad en el intercambio de información

TIPO DE ACTIVO DE INFORMACIÓN	Informacion Impresa																			
AMENAZA	Error operacional del personal			Divulgación no autorizada de información crítica o sensible				Robo o pérdida de información sensible o crítica					Falsificacion			Daños accidentales				Condiciones ambientales adversas
VULNERABILIDAD	Falta / Deficiencia en el procedimiento de identificación, clasificación y manejo de la información	Uso de versiones de documentos desactualizadas	Falta de capacitación de los usuarios	Almacenamiento de información de forma no segura o Inadecuada	Falta / Deficiencia en el procedimiento de identificación, clasificación y manejo de la información	Eliminación de información de forma no segura o Inadecuada	Falta de concientización de los usuarios	Almacenamiento de información de forma no segura o Inadecuada	Eliminación de información de forma no segura o Inadecuada	Falta de concientización de los usuarios	Falta / Deficiencia en el procedimiento de identificación, clasificación y manejo de la información	Falta de seguridad en el intercambio de información	Falta de concientización de los usuarios	Falta de mecanismos de protección de documentos	Falta de capacitación en detección de falsificación de documentos	Almacenamiento de información de forma no segura o Inadecuada	Falta / Deficiencia en el procedimiento de identificación, clasificación y manejo de la información	Mecanismos de intercambio de información no adecuados	Falta de concientización de los usuarios	Almacenamiento de información de forma no segura o Inadecuada

TIPO DE ACTIVO DE INFORMACIÓN	Aplicaciones																									
AMENAZA	Código malicioso			Error de procesamiento				Error operacional del personal			Falla del software					Suplantación de usuarios		Cambios no exitosos en la aplicación		Robo o pérdida de información sensible o crítica					
VULNERABILIDAD	Especificaciones inadecuadas en el diseño e implementación de la aplicación	Falta de gestión de control de cambios	Falta de gestión de vulnerabilidades técnicas	Especificaciones inadecuadas en la definición, diseño e implementación de la aplicación	Falta de criterios/pruebas de aceptación	Deficiencia en los definición de ambientes de desarrollo, prueba y producción	Falta/Falla en la gestión de herramientas y logs de auditoria	Falta / Falla de gestión de capacidad	Falta / desactualización de documentación	Falta / Falla de gestión de acceso de usuarios	Falta de Capacitación de personal	Especificaciones inadecuadas en la definición, diseño e implementación de la aplicación	Falta de gestión de vulnerabilidades técnicas	Falta de gestión de control de cambios	Uso de versiones obsoletas	Falta / pruebas insuficientes de copias de respaldo	Falta / Falla de gestión de acceso de usuarios	Especificaciones inadecuadas en la definición, diseño e implementación de la aplicación	Falta de criterios/pruebas de aceptación	Inexistencia/ Falla en la segregación de ambientes.	Falta/ falla de gestión de acceso de usuarios	Falta de supervisión del trabajo de terceros	Falta de seguridad en el intercambio de información	Falta / Deficiencia en el procedimiento de identificación , clasificación y manejo de la información

TIPO DE ACTIVO DE INFORMACIÓN	Recurso Humano										
AMENAZA	Ausencia repentina		Divulgación no autorizada de información sensible o crítica		Ingenieria social	Robo o pérdida de información sensible crítica					Desastre natural
VULNERABILIDAD	Personal Insatisfecho / desmotivado	Falta de un esquema de respaldo de funciones / conocimiento	Falta de concientización en Seguridad de la Información	Personal Insatisfecho / desmotivado	Falta de concientización en Seguridad de la Información	Falta de concientización en Seguridad de la Información	Falta de Controles de prevencioón de fraude, fuga de información (Medidas disciplinarias inexistentes o inadecuadas)	Falta / Deficiencia en el procedimiento de identifiación , clasificación y manejo de la información	Falta/falla en segregación de funciones	Personal Insatisfecho / desmotivado	Falta de un esquema de respaldo de funciones / conocimiento

TIPO DE ACTIVO DE INFORMACIÓN	Servicio de Tercero							
AMENAZA	Robo / Divulgación no autorizada de información sensible o crítica			Error operacional del personal		Incumplimiento de los acuerdos contractuales			Interrupción repentina del servicio
VULNERABILIDAD	Acuerdos de confidencialidad no existentes o inadecuados	Falta de requerimientos de seguridad en acuerdos contractuales	Falta de concientización de terceros en Seguridad de la Información	Falta / falla de procedimiento de control de cambios	Ausencia de supervisión del trabajo de terceros	Falta de requerimientos de seguridad en acuerdos contractuales	Falta de auditorias del servicio prestado	Ausencia de indicadores de gestión y planes de acción	Plan de continuidad / contingencia

TIPO DE ACTIVO DE INFORMACIÓN	Hardware																							
AMENAZA	Daños accidentales (Aplica para TI y áreas de negocio)		Código malicioso			Error operacional del personal (Aplica solo para TI)				Falla del hardware						Aumento inesperado de las condiciones de operación (Aplica para TI)			Suplantación de usuarios (Aplica para areas de TI y y áreas de negocio)					
VULNERABILIDAD	Ubicación en sitios deficientes en seguridad	Falta/falla de políticas para el trabajo en áreas seguras	Falta/Falla de gestión de herramientas para detección y prevención de código malicioso	Falta/falla de gestión sobre la infraestructura de red	Falta de gestión de vulnerabilidades técnicas	Falta/Desactualización de documentación	Falta/Falla de capacitación de usuarios	Falta/ falla de gestión de control de cambios	Falta / Falla de gestión de acceso de usuarios	Falta/ Gestión inadecuada de herramientas y logs de auditoria	Falta/ falla de gestión de control de cambios	Falta de mantenimiento - lógico o físico	Ausencia/ Falla de Planes de Contingencia	Obsolescencia del Hardware	Falta / Falla de gestión de capacidad	Falta/ Gestión inadecuada de herramientas y logs de auditoria	Falta de Alineación con objetivos del negocio	Falta / Falla de gestión de capacidad	Falta/Falla de concientización de usuarios	Falta / Falla de gestión de acceso de usuarios			

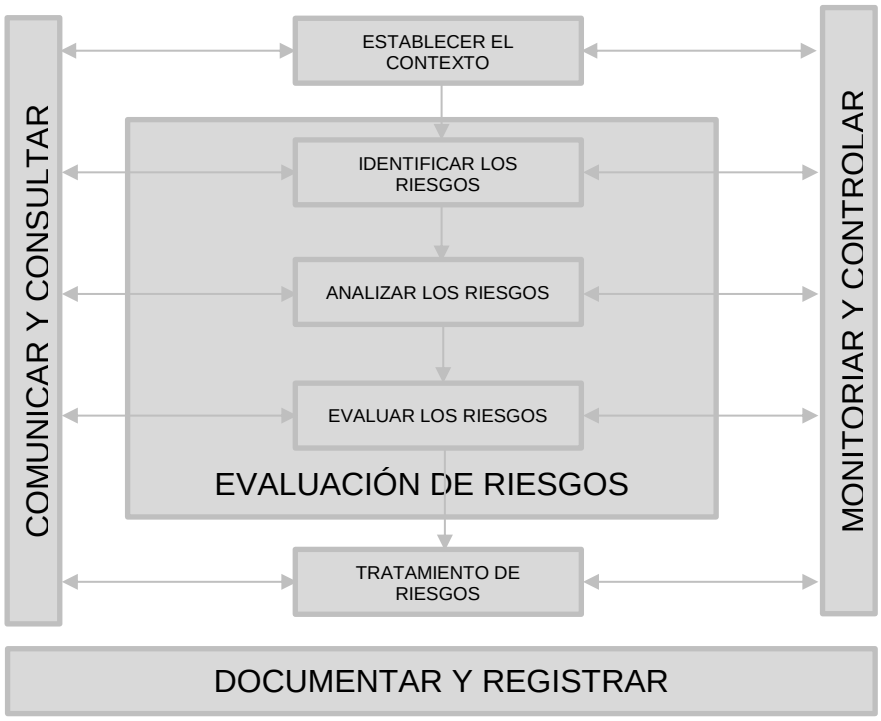
TIPO DE ACTIVO DE INFORMACIÓN	Infraestructura																							
AMENAZA	Acceso no autorizado		Daños accidentales				Incendio		Inundación		Plagas (ratones y cucarachas)	Desastre natural (Terremotos, Huracanes, Tornados, deslizamientos, maremotos, erupciones volcanicas)		Alteraciones de orden público			Acciones Terroristas (Vandalismo , Sabotajes , Bombas, atentados)							
VULNERABILIDAD	Control de acceso inadecuado o inexistente	Falla o falta de políticas de accesos a áreas seguras	Protección Física Inadecuada	Control de acceso inadecuado o inexistente	Sistema de detección y extinción de incendios inadecuado	Falta de mantenimiento de la infraestructura de servicios	Sistema de detección y extinción de incendios inadecuado	Falta de mantenimiento de la infraestructura de servicios	Falta de mantenimiento de la infraestructura de servicios	Ubicación inadecuada de tuberías de agua	Falta de Protección contra plagas	Protección Física Inadecuada	Falta de un plan de continuidad	Protección Física Inadecuada	Sistema de detección y extinción de incendios inadecuado	Esquemas de vigilancia Inadecuados (Servicios de vigilancia , Plan de atención de incidentes)	Protección Física Inadecuada	Ubicación en zonas de alto riesgo					

TIPO DE ACTIVO DE INFORMACIÓN	Enlaces																	
AMENAZA	Daños accidentales			Código malicioso				Error operacional del personal			Falla del hardware				Aumento inesperado de las condiciones de operación		Interceptación de comunicaciones	
VULNERABILIDAD	Ubicación en sitios deficientes en seguridad	Ausencia/ Falla de Planes de Contingencia	Falta/falla de políticas para el trabajo en áreas seguras	Falta/Falla de gestión de herramientas para detección y prevención de código malicioso	Administración Inadecuada de Equipos	Falta/falla de gestión sobre la infraestructura de red	Falta de gestión de vulnerabilidades técnicas	Falta/Desactualización de documentación	Falta/Falla de capacitación de usuarios	Falta / Falla de gestión de acceso de usuarios	Condiciones de instalación y operación inadecuada (eléctrico , instalación de componentes)	Falta de mantenimiento - físico	Obsolescencia del Hardware	Falta / Falla de gestión de capacidad	Falta/ Gestión inadecuada de herramientas y logs de auditoria	Falta / Falla de gestión de capacidad	Falta/falla de mecanismos de cifrado de la comunicación	Falta/falla de gestión sobre la infraestructura de red

TIPO DE ACTIVO DE INFORMACIÓN	Medios Removibles										
AMENAZA	Robo o Pérdida de informacion sensible o crítica					Divulgación no autorizada de información crítica o sensible			Daños accidentales	
VULNERABILIDAD	Almacenamiento del medio de forma no segura o Inadecuada	Falta de mecanismos de encripción de datos	Falta de procedimiento de desecho /reutilización de medios	Falta de seguridad en el intercambio de información	Falta de concientización de los usuarios	Almacenamiento del medio de forma no segura o Inadecuada	Falta / Deficiencia en el procedimiento de identificación y clasificación de la información	Falta de política de escritorio limpio	Almacenamiento del medio de forma no segura o Inadecuada	Transporte idanecuado de los medios de almacenamiento

6. PROCESO DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Basados en la norma ISO 27005, la GOBERNACIÓN DE BOLÍVAR, ejecutará el siguiente modelo de gestión de riesgos, el cual ayudará a garantizar un tratamiento adecuado de los riesgos de seguridad de la información:



Modelo de gestión de riesgos de seguridad de la información. NTC/ISO 27005

6.1 ESTABLECER EL CONTEXTO

Definir los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la GOBERNACIÓN DE BOLÍVAR y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos.

6.2 EVALUACIÓN DE RIESGOS

Identificar los activos de información por proceso en evaluación. Conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de

información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto.

6.2.1 Identificar riesgo

Tiene como objetivo conocer los escenarios que pueden producir en la entidad y los efectos que puedan tener sobre los objetivos de esta.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

6.2.2 Analizar riesgo

Permite determinar la severidad de este a partir del impacto y la probabilidad de su ocurrencia, así como también determinar el riesgo inherente de cada activo y asignar el responsable.

La probabilidad dirá cuál puede ser la ocurrencia del riesgo y el impacto inherente en la Gobernación de Bolívar sin tener presente los controles al materializarse, por lo que debe verse en el peor de los escenarios posibles.

6.2.2.1 Probabilidad

Valor	Nivel	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales y/o la eficacia de los controles es alta.	No se ha presentado en los últimos 4 años
3	Posible	El evento podría ocurrir en algún momento y/o la eficacia de los controles es baja.	Al menos una vez en los últimos 2 años
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias y/o no existen controles o si existen es nula su eficacia.	Más de una vez al año

6.2.2.2 Impacto

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		Impacto (Consecuencias) Cuantitativo	Impacto (Consecuencias) Cualitativo
INSIGNIFICANTE	1	Afectación >=X% de la población. Afectación >=X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación >=X% de la población. Afectación >=X% del presupuesto anual de la entidad. Afectación leve del medio ambiente Requiere >=%X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación >=X% de la población. Afectación >=X% del presupuesto anual de la entidad. Afectación leve del medio ambiente Requiere >=%X semanas de recuperación.	Afectación moderada de la integridad de la información, debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información, debido al interés particular de los empleados y terceros. Afectación moderada de la integridad de la confidencialidad, debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación >=X% de la población. Afectación >=X% del presupuesto anual de la entidad. Afectación importante del medio ambiente Requiere >=%X semanas de recuperación.	Afectación grave de la integridad de la información, debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información, debido al interés particular de los empleados y terceros. Afectación grave de la integridad de la confidencialidad, debido al interés particular de los empleados y terceros.

Fuente: Equipo Riesgos Gobernación de Bolívar - Min TIC

6.2.3 Evaluar riesgo

PROBABILIDAD	IMPACTO		
	Bajo (1)	Medio (3)	Alto (5)
Raro (1)	1	3	5
Posible (3)	3	9	15
Casi Seguro (5)	5	15	25

Igual a 1: zona de riesgo baja: asumir el riesgo.
Mayor a 1 menor a 9: zona de riesgo moderada: asumir el riesgo, reducir el riesgo.
Mayor o igual a 9: zona de riesgo alta: reducir el riesgo, evitar, compartir o transferir.

6.3 TRATAMIENTO DE RIESGOS

Seleccionar una opción de tratamiento basados en la evaluación de riesgos:

✓ **Evitar el riesgo:** su propósito es no proceder con la actividad o la acción que da origen al riesgo.
✓ **Transferir o compartir el riesgo:** entregando la gestión del riesgo a un tercero.
✓ **Reducir o Mitigar el riesgo**: seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
✓ **Retener o aceptar el riesgo**: no se tomará la decisión de implementar medidas de control adicionales. Será monitoreado para confirmar que no se incrementa.

6.3.1 Controles

5	POLITICAS DE SEGURIDAD	
5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
5.1.1	Políticas para la seguridad de la información	
5.1.2	Revisión de las políticas para la seguridad de la información	
6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
6.1	**Organización interna**	
6.1.1	Roles y responsabilidades para la seguridad de información	
6.1.2	Separación de deberes	
6.1.3	Contacto con las autoridades	

6.1.4	Contacto con grupos de interés especial	
6.1.5	Seguridad de la información en la gestión de proyectos	
6.2	**Dispositivos móviles y teletrabajo**	
6.2.1	Política para dispositivos móviles	
6.2.2	Teletrabajo	
7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	
7.1	**Antes de asumir el empleo**	
7.1.1	Selección	
7.1.2	Términos y condiciones del empleo	
7.2	**Durante la ejecución del empleo**	
7.2.1	Responsabilidades de la dirección	
7.2.2	Toma de conciencia, educación y formación en la seguridad y privacidad de la información.	
7.2.3	Proceso disciplinario	
7.3	**Terminación o cambio de empleo**	
7.3.1	Terminación o cambio de responsabilidades de empleo	
8	**GESTIÓN DE ACTIVOS**	
8.1	**Responsabilidad sobre los activos**	
8.1.1	Inventario de activos	
8.1.2	Propiedad de los activos	
8.1.3	Uso aceptable de los activos	
8.1.4	Devolución de activos	
8.2	**Clasificación de la Información**	
8.2.1	Clasificación de la información	
8.2.2	Etiquetado de la información	
8.2.3	Manejo de activos	
8.3	**Manejo de medios**	
8.3.1	Gestión de medios removibles	
8.3.2	Disposición de los medios	
8.3.3	Transferencia de medios físicos	
9	**CONTROL DE ACCESO**	
9.1	**Requisitos de negocio para el control de acceso**	
9.1.1	Política de control de acceso	
9.1.2	Acceso a las redes y servicios en red	
9.2	**Gestión de acceso de usuarios**	
9.2.1	Registro y cancelación del registro de usuarios	
9.2.2	Suministro de acceso de usuarios	
9.2.3	Gestión de derechos de acceso privilegiado	
9.2.4	Gestión de información de autenticación secreta de usuarios	
9.2.5	Revisión de los derechos de acceso de los usuarios	

9.2.6	Retiro o ajuste de los derechos de acceso	
9.3	**Responsabilidades de los usuarios**	
9.3.1	Uso de la información de autenticación secreta	
9.4	**Control de acceso a sistemas y aplicaciones**	
9.4.1	Restricción del acceso a la información	
9.4.2	Procedimiento de ingreso seguro	
9.4.3	Sistema de gestión de contraseñas	
9.4.4	Uso de programas utilitarios privilegiados	
9.4.5	Control de acceso al código fuente de los programas	
10	**CRIPTOGRAFÍA**	
10.1	**Controles criptográficos**	
10.1.1	Política sobre el uso de controles criptográficos	
10.1.2	Gestión de llaves	
11	**SEGURIDAD FíSICA Y DEL ENTORNO**	
11.1	**Áreas Seguras**	
11.1.1	Perímetro de seguridad física	
11.1.2	Controles físicos de entrada	
11.1.3	Seguridad de oficinas, recintos e instalaciones	
11.1.4	Protección contra las amenazas externas y ambientales	
11.1.5	Trabajo en áreas seguras	
11.1.6	Áreas de despacho y carga	
11.2	**Equipos**	
11.2.1	Ubicación y protección de los equipos	
11.2.2	Servicios de suministro	
11.2.3	Seguridad del cableado	
11.2.4	Mantenimiento de los equipos	
11.2.5	Retiro de activos	
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	
11.2.7	Disposición segura o reutilización de equipos	
11.2.8	Equipos de usuario desatendidos	
11.2.9	Política de escritorio limpio y pantalla limpia	
12	**SEGURIDAD DE LAS OPERACIONES**	
12.1	**Procedimientos operacionales y responsabilidades**	
12.1.1	Procedimientos de operación documentados	
12.1.2	Gestión de cambios	
12.1.3	Gestión de capacidad	
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	
12.2	**Protección contra código malicioso**	
12.2.1	Controles contra el código malicioso.	

12.3	**Copias de seguridad**	
12.3.1	Copias de seguridad de la información	
12.4	**Registro y seguimiento**	
12.4.1	Registro de eventos	
12.4.2	Protección de la información de registro	
12.4.3	Registros del administrador y del operador	
12.4.4	Sincronización de relojes	
12.5	**Control de software operacional**	
12.5.1	Instalación de software en sistemas operativos	
12.6	**Gestión de la vulnerabilidad técnica**	
12.6.1	Gestión de las vulnerabilidades técnicas	
12.6.2	Restricciones sobre la instalación de software	
12.7	**Consideraciones sobre auditorias de sistemas de información**	
12.7.1	Controles de auditorías de sistemas de información	
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	
13.1	**Gestión de la seguridad en las redes**	
13.1.1	Controles de red	
13.1.2	Seguridad de los servicios de red.	
13.1.3	Segregación de redes	
13.2	**Transferencia de información**	
13.2.1	Políticas y procedimientos de intercambio de información	
13.2.2	Acuerdos sobre transferencia de información	
13.2.3	Mensajería electrónica	
13.2.4	Acuerdos de confidencialidad o de no divulgación	
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**	
14.1	**Requisitos de seguridad de los sistemas de información**	
14.1.1	Análisis y especificación de requisitos de seguridad de la información	
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	
14.1.3	Protección de transacciones de los servicios de las aplicaciones	
14.2	**Seguridad en los procesos de desarrollo y soporte**	
14.2.1	Política de desarrollo seguro	
14.2.2	Procedimientos de control de cambios en sistemas	
14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	
14.2.4	Restricciones en los cambios a los paquetes de software	
14.2.5	Principios de construcción de sistemas seguros	
14.2.6	Ambiente de desarrollo seguro	
14.2.7	Desarrollo contratado externamente	
14.2.8	Pruebas de seguridad de sistemas	
14.2.9	Pruebas de aceptación de sistemas	

14.3	**Datos de prueba**	
14.3.1	Protección de datos de prueba	
15	**RELACIÓN CON PROVEEDORES**	
15.1	**Seguridad de la información en las relaciones con los proveedores**	
15.1.1	Política de seguridad de la información para las relaciones con proveedores	
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	
15.1.3	Cadena de suministro de tecnología de información y comunicación	
15.2	**Gestión de la prestación de servicios con los proveedores**	
15.2.1	Seguimiento y revisión de los servicios de los proveedores	
15.2.2	Gestión de cambios en los servicios de proveedores	
16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	
16.1	**Gestión de incidentes y mejoras en la seguridad de la información**	
16.1.1	Responsabilidad y procedimientos	
16.1.2	Reporte de eventos de seguridad de la información	
16.1.3	Reporte de debilidades de seguridad de la información	
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	
16.1.5	Respuesta a incidentes de seguridad de la información	
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	
16.1.7	Recolección de evidencia	
17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**	
17.1	**Continuidad de seguridad de la información**	
17.1.1	Planificación de la continuidad de la seguridad de la información	
17.1.2	Implementación de la continuidad de la seguridad de la información	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	
17.2	**Redundancias**	
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	
18	**CUMPLIMIENTO**	
18.1	**Cumplimiento de requisitos legales y contractuales**	
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	
18.1.2	Derechos de propiedad intelectual	
18.1.3	Protección de registros	
18.1.4	Privacidad y protección de datos personales	
18.1.5	Reglamentación de controles criptográficos	
18.2	**Revisiones de seguridad de la información**	
18.2.1	Revisión independiente de la seguridad de la información	
18.2.2	Cumplimiento con las políticas y normas de seguridad	
18.2.3	Revisión del cumplimiento técnico	

Controles - ISO/IEC 27002:2013