Plan

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GTE-PL-03-V2

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
31-01-2020

Tabla de Contenido

1. PROPÓSITO

Gestión de riesgos: propósito. Definir una metodología que permita a la entidad establecer un conjunto de actividades y tareas que faciliten la identificación y gestión de los riesgos de seguridad y privacidad de la información, y así mismo mitigar la materialización de amenazas que afecten los activos de información de la UNP.

2. OBJETIVO

1. Adoptar los lineamientos del marco de referencia relacionados con el tratamiento de riesgos de seguridad y privacidad de la información.
2. Elaborar un plan tratamiento de riesgos de seguridad que permita a la UNP preservar la confidencialidad, integridad y disponibilidad de su información.
3. Definir e implementar las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
4. Alinear el plan de tratamiento de riesgos de seguridad con los planes institucionales, y la normatividad prevista por MSPI del MinTic y la ISO 27001

3. ALCANCE

Tiene en cuenta y adopta recomendaciones y lineamientos de la metodología de gestión de riesgos, en especial los de seguridad y privacidad de la información de acuerdo con los documentos:

- Guía 7 - Gestión de Riesgos del MinTic

- Guía 8 - Controles de Seguridad respectivamente del MinTic.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas: riesgos de gestión, corrupción y seguridad digital de la Función Pública.
- Anexo A del marco de gestión de seguridad de la norma ISO 27001.

Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital.

4. DEFINICIONES

Los términos establecidos a continuación son tomados de la Guía Técnica del MinTic, la norma técnica ISO 27001 y la Guía para la Administración del Riesgo del DAFP.
Los tres (3) pilares de la información: confidencialidad, integridad y disponibilidad de la información.

- *Confidencialidad de la información*: la información solo debe ser accesible por los destinatarios determinados autorizados.
- *Integridad de la información:* la información debe ser correcta y estar completa.
- *Disponibilidad de la información*: la información debe estar disponible y accesible para su tratamiento en el momento y lugar que se requiera.

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
Activo de Información: cualquier información, sistema de información o infraestructura tecnológica relacionada con el tratamiento de esta que tenga valor para la Entidad.

Ejemplos de activos de información: información, bases de datos, software, hardware, contratos, equipos de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales (calefacción, iluminación, energía, aire acondicionado), y las personas que son quienes generan, transmiten y destruyen información.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Consecuencia: os efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de gestión: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. RESPONSABILIDADES

Se definen los responsables del Plan de Tratamiento de Riesgos de seguridad y privacidad de la información dentro de la Unidad Nacional de Protección, como parte del Modelo de Seguridad y Privacidad de la Información, así:

Responsables del documento:

1º Oficial de Seguridad de la Información.

Grupo de Gestión de Tecnologías de la Información

2º. Coordinador de Tecnología.

Grupo de Gestión de Tecnologías de la Información.

3º. CIO del Grupo de Tecnología

Grupo de Gestión de Tecnologías de la Información

6. MARCO LEGAL

INTEGRACIÓN DE PLANES DE MIPG

Teniendo en cuenta lo dispuesto en el Decreto 612 de 2018 respecto a la integración de planes institucionales y estratégicos al plan de acción, el presente documento desarrolla la siguiente actividad descrita en el Plan de Acción 2019: "Adoptar las guías del sistema de gestión de seguridad de información - SGSI del modelo de seguridad y privacidad de la información - MSPI del MinTic en la UNP", del cual se presentará el producto "Documento informe de seguimiento de implementación del sistema de gestión de seguridad de la información.".

7. CONTENIDO

7.1 Requisitos

7.2 Compromiso de la alta gerencia para promover, apoyar y financiar la realización de los proyectos asociados a gestionar los riesgos de seguridad de la información.

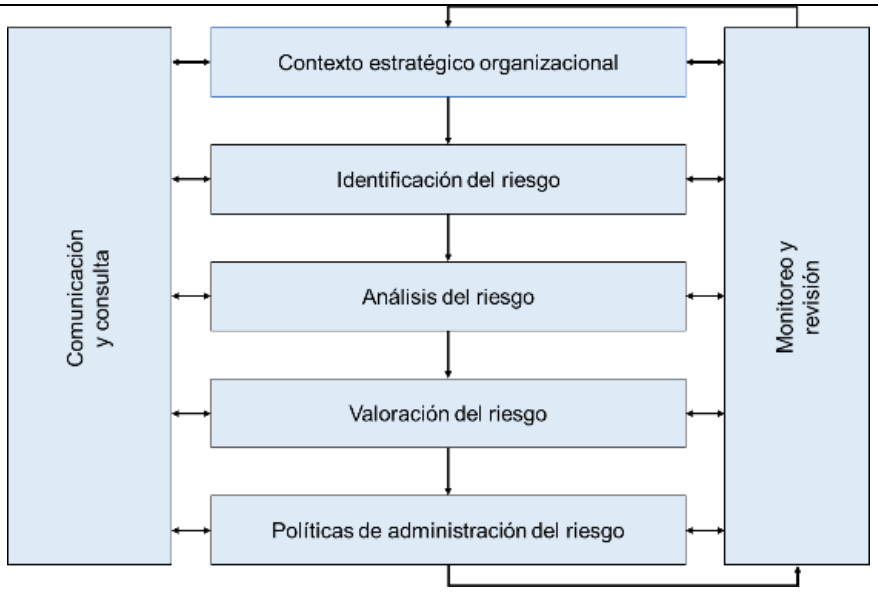
7.3 Integración de los riesgos de seguridad de la información al marco de gestión de riesgos de la UNP por parte de la Oficina Asesora de Planeación e Información.

7.4 Adopción de la cultura de seguridad de la información y compromiso de todos los colaboradores y grupos de interés de la UNP frente los riesgos de seguridad de la información y su tratamiento.

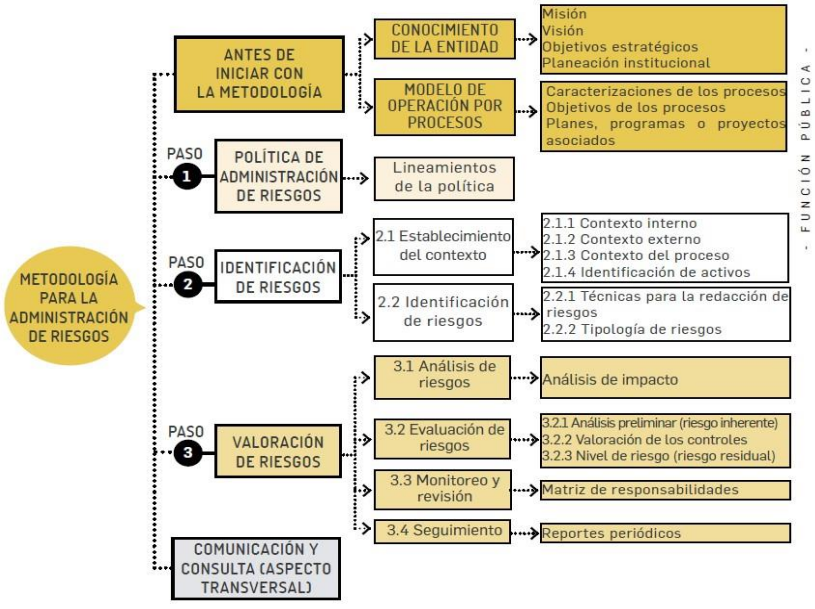
7.5 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

7.5.1 Etapas para la Gestión del Riesgo.

De acuerdo con la Guía de Gestión de Riesgos del DAFP – Departamento Administrativo de la Función Pública, las etapas generales para la gestión de riesgos aplicados en la UNP contemplan el compromiso de la dirección de la Entidad, el equipo interdisciplinario encargado de la administración del modelo de gestión de riesgos y las capacitaciones de la metodología, lo cual está a cargo de la Oficina Asesora de Planeación e Información.



Proceso para la administración del riesgo - DAFP



Metodología para la administración de riesgos del DAFP

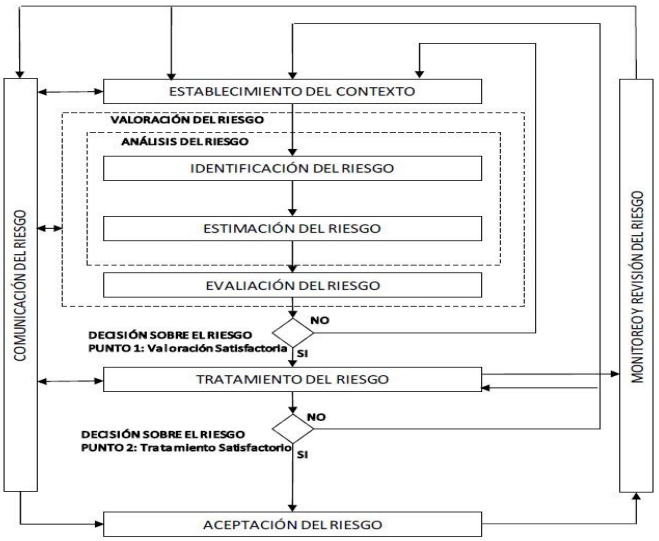
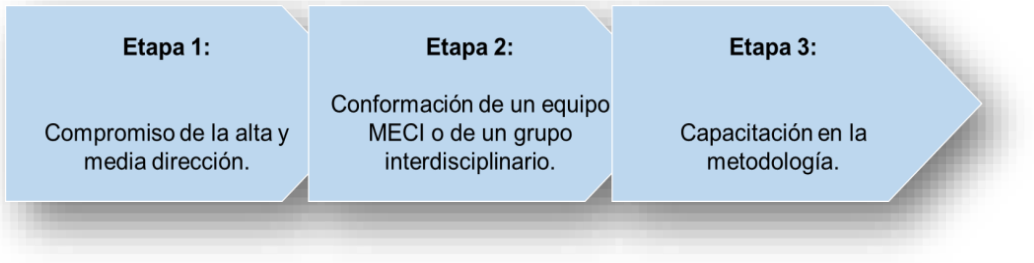


Imagen 2. Tomado de la NTC-ISO/IEC 27005

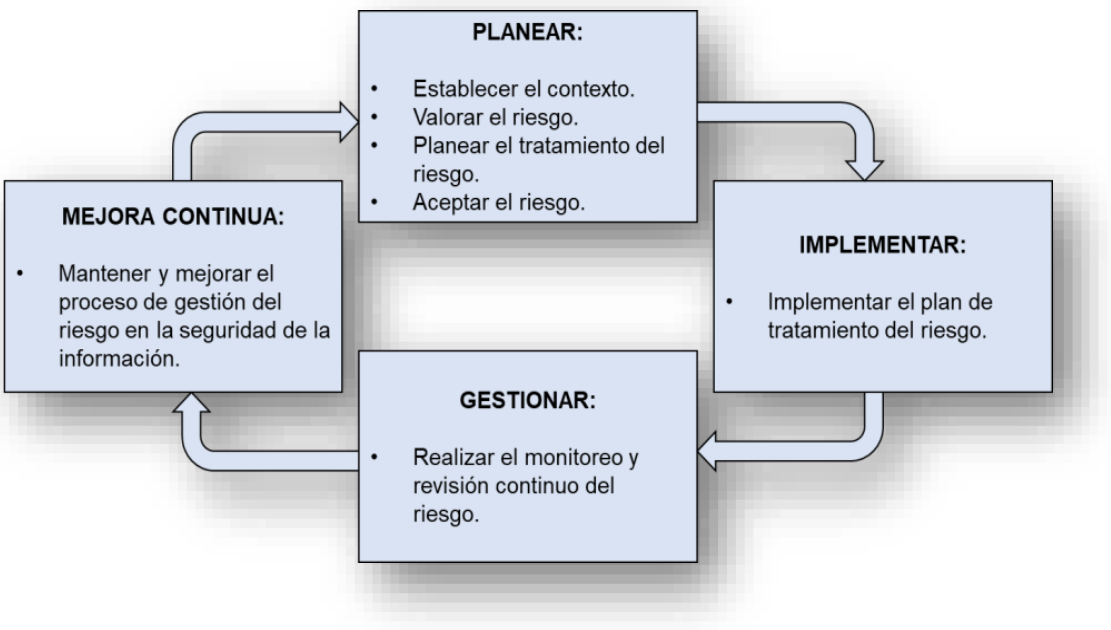
Proceso para la administración del riesgo en seguridad de la información – ISO 27005



7.5.2 Visión general para la Administración del Riesgo.

Para el establecimiento de el plan de tratamiento de riesgos de seguridad y privacidad de la información de la UNP, el Grupo de Tecnología revisó diferentes metodologías, entre las cuales están el proceso y la metodología de administración de riesgos del DAFP, y el proceso para la administración del riesgo en seguridad de la información de la ISO 27005, de los cuales tomamos la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento al interior de la UNP.

A continuación, se presentan las subactividades a ejecutar de gestión del riesgo a lo largo del MSPI – Modelo de Seguridad y Privacidad de la Información:



7.5.3 Criterios a tener en cuenta en la Implementación de la Metodología de Gestión de Riesgos de Seguridad y Privacidad de la Información.

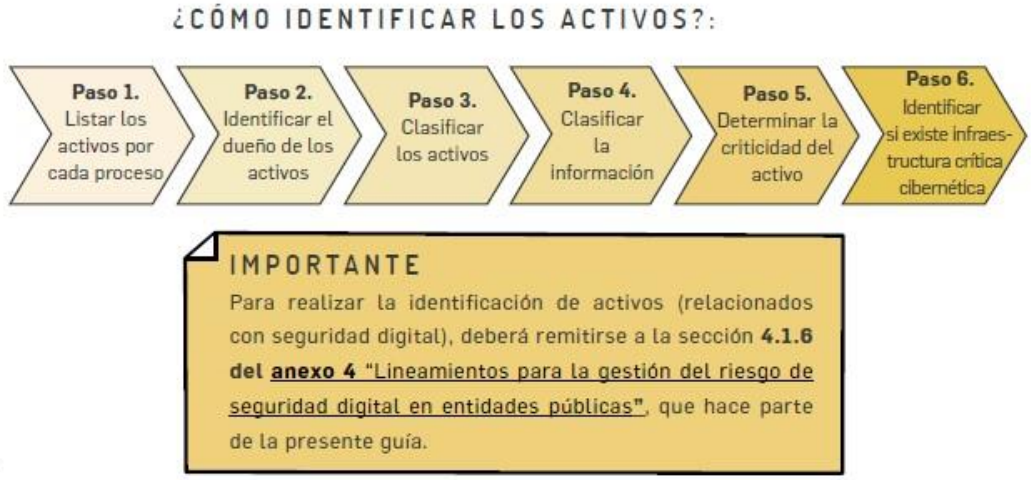
Factores de riesgo por cada categoría del contexto según DAFP:

CONTEXTO	FACTORES
CONTEXTO EXTERNO	POLÍTICOS: cambios de gobierno, legislación, políticas públicas, regulación.
	ECONÓMICOS Y FINANCIEROS: disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	SOCIALES Y CULTURALES: demografía, responsabilidad social, orden público.

	TECNOLÓGICOS: avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
CONTEXTO	**FACTORES**
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.

	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS: pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS: efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Identificación de activos – DAFP:

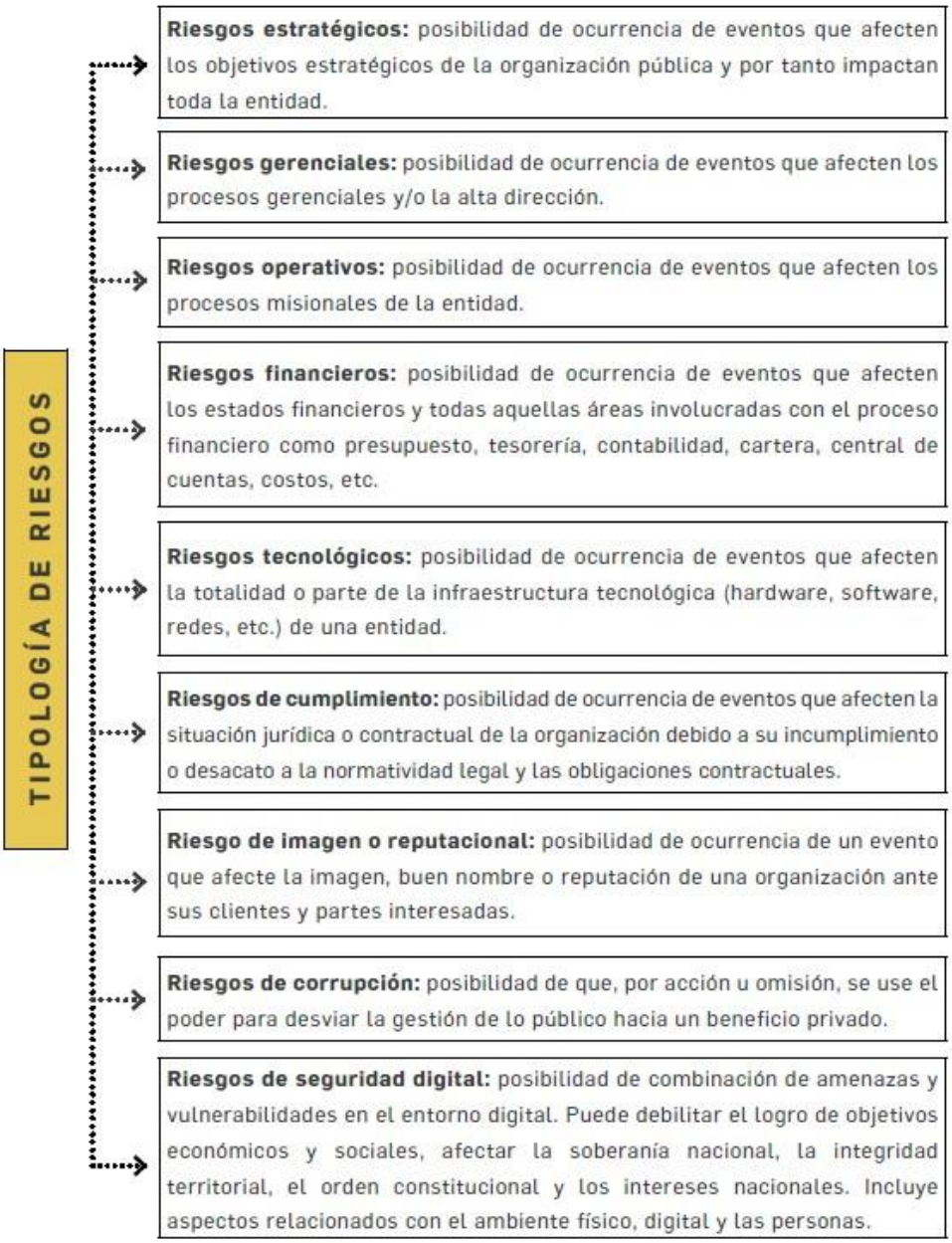


Tipos de activos:

Información	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
Software:	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas
Recurso humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

Servicio	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet
Hardware	Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos
Otros	activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso

Tipología de riesgos – DAFP:


TIPOLOGÍA DE RIESGOS
Riesgos estratégicos: posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
Riesgos gerenciales: posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos operativos: posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos financieros: posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos tecnológicos: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de cumplimiento: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
Riesgos de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos de seguridad digital: posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Clasificación de activos:

CLASIFICACIÓN					
CONFIDENCIALIDAD		INTEGRIDAD		DISPONIBILIDAD	
INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.	A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.	1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por	M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen	2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad

	todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario		moderado a funcionarios de la entidad.		
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.	B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.	3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA	NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA	NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

Criterios para calificar la probabilidad – DAFP:

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Criterios para calificar el impacto en riesgos de seguridad digital – DAFP:

Nivel	Valor del impacto	Impacto cuantitativo	Impacto 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 de ≥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 de ≥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 confidencialidad de la información debido al interés particular de los empleados y terceros.

Nivel	Valor del impacto	Impacto cuantitativo	Impacto cualitativo
Mayor	4	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • Afectación importante del medio ambiente que requiere de ≥X meses 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 confidencialidad de la información debido al interés particular de los empleados y terceros.

catastrófico	5	• Afectación ≥X% de la población. • Afectación ≥X% del presupuesto anual de la entidad. • Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	• Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. • Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Identificación de amenazas**:**

FUENTES DE AMENAZAS HUMANAS		
FUENTE DE LA AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
PIRATA INFORMÁTICO, INTRUSO ILEGAL	RETO, EGO, REBELIÓN, ESTATUS, DINERO	PIRATERÍA, INGENIERÍA SOCIAL, INTRUSIÓN, ACCESOS FORZADOS AL SISTEMA, ACCESO NO AUTORIZADO.
CRIMINAL DE LA COMPUTACIÓN	DESTRUCCIÓN DE LA INFORMACIÓN, DIVULGACIÓN ILEGAL DE LA INFORMACIÓN, GANANCIA MONETARIA, AUTORIZACIÓN NO AUTORIZADA DE LOS DATOS	CRIMEN POR COMPUTADOS, ACTO FRAUDULENTO, SOBORNO DE LA INFORMACIÓN, SUPLANTACIÓN DE LA IDENTIDAD, INTRUSIÓN EN EL SISTEMA
TERRORISMO	CHANTAJE, DESTRUCCIÓN, EXPLOTACIÓN, VENGANZA, GANANCIA POLÍTICA, CUBRIMIENTO DE LOS MEDIOS DE COMUNICACIÓN	BOMBA, TERRORISMO, GUERRA DE LA INFORMACIÓN, ATAQUES CONTRA EL SISTEMA DDOS, PENETRACIÓN EN EL SISTEMA, MANIPULACIÓN EN EL SISTEMA
ESPIONAJE INDUSTRIAL: INTELIGENCIA, EMPRESAS, GOBIERNOS, EXTRANJEROS, OTROS INTERESES	VENTAJA COMPETITIVA, ESPIONAJE ECONÓMICO,	VENTAJA DE DEFENSA, VENTAJA POLÍTICA, EXPLOTACIÓN ECONÓMICA, HURTO DE INFORMACIÓN, INTRUSIÓN EN PRIVACIDAD PERSONAL, INGENIERÍA

		SOCIAL, PENETRACIÓN EN EL SISTEMA, ACCESO NO AUTORIZADO EN EL SISTEMA
INTRUSOS: EMPLEADOS CON ENTRENAMIENTO DEFICIENTE, DESCONTENTOS, MALINTENCIONADOS, NEGLIGENTES, DESHONESTOS, DESPEDIDOS.	CURIOSIDAD, EGO, INTELIGENCIA, GANANCIA MONETARIA, VENGANZA, ERRORES Y OMISIONES NO INTENCIONALES (ERROR EN EL INGRESO DE DATOS, ERROR EN LA PROGRAMACIÓN)	ASALTO A UN EMPLEADO, CHANTAJE, OBSERVAR INFORMACIÓN RESERVADA, USO INADECUADO DEL COMPUTADOR, FRAUDE Y HURTO, SOBORNO DE INFORMACIÓN, INGRESO DE DATOS FALSOS O CORRUPTOS, INTERCEPTACIÓN, CÓDIGO MALICIOSO, VENTA DE INFORMACIÓN PERSONAL, ERRORES EN EL SISTEMA, INTRUSIÓN AL SISTEMA, SABOTAJE DEL SISTEMA

FUENTES DE AMENAZAS HUMANAS		
FUENTE DE LA AMENAZA	MOTIVACIÓN	ACCIONES AMENAZANTES
		ACCESO NO AUTORIZADO AL SISTEMA

Relación de vulnerabilidades y amenazas por tipo de activo:

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final	Hurtos medios o documentos.
	Copia no controlada	Hurtos medios o documentos.

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	Abuso de los derechos

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos

	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
RED	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones

	Punto único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del de sistema información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos

	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
ORGANIZACIÓN	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de	Abuso de los derechos

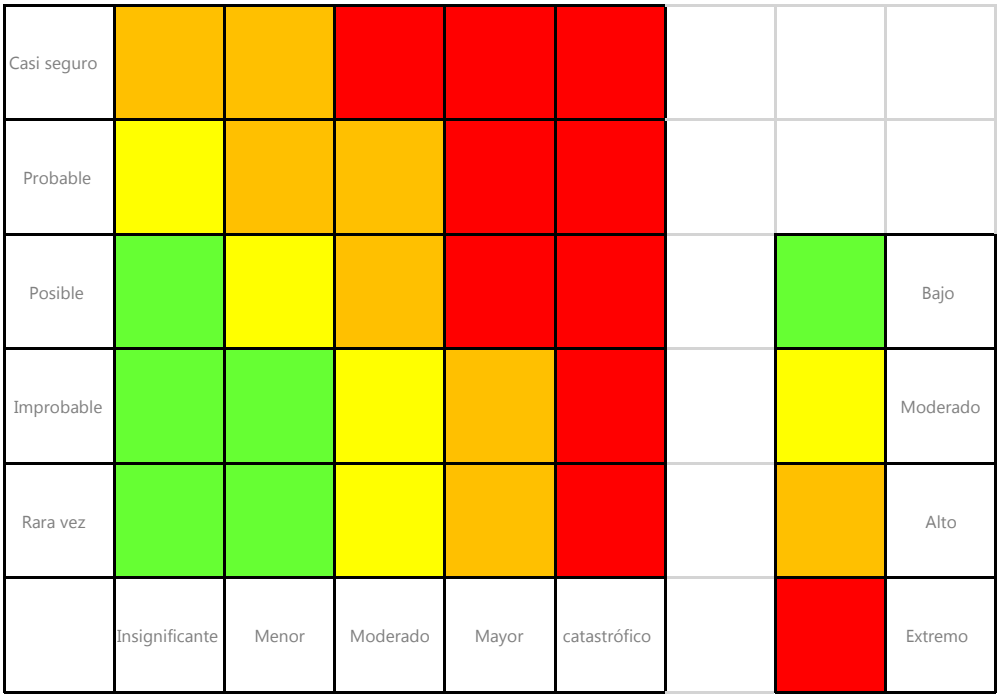
	procesamiento de la información	
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso

Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo

TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado

Nivel de riesgo por relación de probabilidad de ocurrencia con impacto – DAFP:



7.6 Plan de Implementación.

El desarrollo de las etapas de gestión de riesgos se ejecutará con la estructura y subactividades recomendadas por el Modelo de Seguridad y Privacidad de la Información. El plan de trabajo contempla la realización de las siguientes subactividades, las cuales deberán incorporarse a la metodología de la UNP de gestión de riesgos, que actualmente tiene los riesgos de corrupción y los de proceso.

Subactividades:

Planear	Implementar	Gestionar	Mejora continúa	Subactividades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
x				Establecer el contexto	x											
x				Valorar el riesgo		x										
x				Planear el tratamiento del riesgo		x										
x				Aceptar el riesgo		x										
	x			Implementar el plan de tratamiento de riesgos		x	x	x	x	x	x	x	x	x	x	X
		x		Realizar el monitoreo y revisión continuo del riesgo			x			x			x			X
			x	Mantener y mejorar el proceso de gestión de riesgo en la seguridad de la información			x			x			x			X

Estructura:

Subactividades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Políticas de administración del riesgo	x											
Contexto estratégico	x											

Identificación del riesgo		x										
Identificación de activos		x										
Identificación de amenazas		x										
Identificación de vulnerabilidades		x										
Estimación del riesgo		x										
Evaluación del riesgo		x										

Subactividades	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Tratamiento del riesgo		x	x	x	x	x	x	x	x	x	x	X
Aceptación del riesgo		x										
Monitoreo y revisión			x			x			x			X
Seguimiento			x			x			x			X
Valoración de controles			x			x			x			X
Estructura de controles	x											
Plan implementación controles		x										

Riesgos para tratar en la vigencia 2020:

RIESGOS	CAUSAS

R1	Afectación de la operación de la entidad por falta de ejecución de los proyectos tecnológicos definidos en el PETI (Plan Estratégico de las Tecnologías de Información).	• Deficiente gestión de los riesgos asociados a los proyectos tecnológicos definidos en el PETI • Insuficiente recurso humano para la estructuración y gestión de proyectos de TI • Falta de apoyo de la Alta Dirección en la implementación de proyectos tecnológicos
R2	Inoportunidad e inefectividad en la prestación de servicios de mesa de ayuda de TI	• Inadecuada gestión del Proceso Gestión Tecnológica para incorporar los Acuerdos de Nivel de Servicios - ANS en el diseño, ejecución y control en la prestación de los servicios tecnológicos. • Falta de mecanismo de seguimiento y control para la ejecución del mantenimiento preventivo y correctivo de la plataforma tecnológica e informática de la Entidad. • Desactualización del alcance de los servicios tecnológicos existentes. • Necesidad de incorporar nuevos servicios tecnológicos.

R3	Afectación de la operación de la Entidad por pérdida de disponibilidad y continuidad de los servicios de TI	• Indisponibilidad de los servicios tecnológicos por falta de la capacidad de la plataforma tecnológica o fallas en los procesos de mantenimiento de la infraestructura que afectan los servicios tecnológicos. • Falta de articulación de todos los procesos con tecnología para establecer procedimientos que identifiquen los activos y servicios que deban contar con planes de contingencia y continuidad. • Falta de actualizaciones en la plataforma de los servicios de TI de la entidad.
R4	Suministro, divulgación o alteración de información reservada, clasificada, sensible o privilegiada de la entidad, para uso indebido en beneficio propio o de un tercero.	• Fuga de información derivada de motivaciones personales (funcionarios y colaboradores inconformes) o de terceros • Mecanismos de control débiles respecto a la identificación, clasificación y uso de activos de información. • Falta de contenidos enfocados en la seguridad y tratamiento de la información, así como las resposnsabildades derivadas para los usuarios en el Plan de Sensibilización

		• No se cuenta con documentos formalizados que definan los roles y responsablidades relacionados con la seguridad y privacidad de la informacion de la entidad.

Tratamiento:

RIESGOS		MONITOREO Y REVISIÓN	
		Acciones	Responsables
R1	Afectación de la operación de la entidad por falta de ejecución de los proyectos tecnológicos definidos en el PETI (Plan Estratégico de las Tecnologías de Información).	1. Definir líneas de seguimiento y control para la ejecución de los proyectos tecnológicos incluidos en el PETI a fin de gestionar los riesgos asociados 2. Solicitar el personal con las competencias requeridas para la estructuración y gestión de los proyectos de TI definidos en el PETI ante la instancia competente 3. Socializar a la Alta Dirección sobre la metodología de estructuración del PETI y su actualización para la vigencia 2020	CIO, Coordinador GGTI, Gestor de Proyectos de TI y Arquitectura Empresarial y equipos de trabajo

R2	Inoportunidad e inefectividad en la prestación de servicios de mesa de ayuda de TI	1. Realizar seguimiento en la Herramienta de gestión de la mesa de ayuda de TI (Centro de Servicios), sobre atención y el cumplimiento de los ANS establecidos en el Catálogo de Servicios 2. Ejecutar el Plan de Mantenimiento preventivo y correctivo de la Infraestructura Tecnológica de la Entidad de acuerdo a los términos establecidos en el mismo. 3. Realizar periódicamente las actividades de revisión y actualización del Catalogo de Servicios Tecnológicos de la Entidad	CIO, Coordinador GGTI , lideres de servicio y Gestor de Proveedores de productos y servicios de TI
R3	Afectación de la operación de la Entidad por pérdida de disponibilidad y continuidad de los servicios de TI	1. Realizar seguimiento y monitoreo a la disponibilidad y capacidad de los servicios tecnológicos, a través de los mecanismos establecidos en la gestión de capacidad documentada. 2. Realizar actividades de generación e implementación de lineamientos sobre la habilitación tecnológica de los procesos en la gestión de activos de información y la protección de los mismos.	(Compartido o transferido) CIO, Coordinador GGTI y Líder a cargo del Proceso de Gestión documental, DBA y gestores de servicios de TI

		3. Actualizar la plataforma de servicios de TI de la entidad de acuerdo a los lineamientos establecidos en los mapas de servicio.de TI	
R4	Suministro, divulgación o alteración de información reservada, clasificada, sensible o privilegiada de la entidad, para uso indebido en beneficio propio o de un tercero.	1. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales. 2. Implementar controles para los activos de información identificados y clasificados. 3. Definir los roles y responsabilidades relacionados con la seguridad de la información.	CIO - CISO, Coordinador GGTI y Lideres de Servicios de TI

TABLA DE CONTROLES PARA MITIGAR LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para el tratamiento, se debe revisar, y analizar la declaración de aplicabilidad de los controles de seguridad establecidos en el Anexo A de la norma ISO 27001:2013.

A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**	
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.		
A.5.1.1	Políticas para la seguridad de la información	*Control* Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control* Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	
A.6.1	**Organización interna**	
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control* Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	*Control* Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	*Control* Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	*Control*

		Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	*Control* La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2 Dispositivos móviles y teletrabajo		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.		
A.6.2.1	Política para dispositivos móviles	*Control* Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	*Control* Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1 Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.		
A.7.1.1	Selección	*Control* Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	*Control* Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

A.7.2 Durante la ejecución del empleo		
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.		
A.7.2.1	Responsabilidades de la dirección	*Control* La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	*Control* Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	*Control* Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3 Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	*Control* Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
A.8 GESTIÓN DE ACTIVOS		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.		

A.8.1.1	Inventario de activos	*Control* Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	*Control* Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	*Control* Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	*Control* Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.		
A.8.2.1	Clasificación de la información	*Control* La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	*Control* Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	*Control* Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

A.8.3 Manejo de medios		
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.		
A.8.3.1	Gestión de medios removibles	*Control* Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	*Control* Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	*Control* Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9 CONTROL DE ACCESO		
A.9.1 Requisitos del negocio para control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	*Control* Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	*Control* Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2 Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.		
A.9.2.1	Registro y cancelación del registro de usuarios	*Control* Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

A.9.2.2	Suministro de acceso de usuarios	*Control* Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	*Control* Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	*Control* La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	*Control* Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	*Control* Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
A.9.3	**Responsabilidades de los usuarios**	
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	*Control* Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**	
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

A.9.4.2	Procedimiento de ingreso seguro	*Control* Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	*Control* Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	*Control* Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	*Control* Se debe restringir el acceso a los códigos fuente de los programas.
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	*Control* Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	*Control* Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1 Áreas seguras		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.		

A.11.1.1	Perímetro de seguridad física	*Control* Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos	*Control* Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control* Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control* Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	*Control* Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	*Control* Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

A.11.2 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	*Control* Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

A.11.2.2	Servicios de suministro	*Control* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	*Control* El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño
A.11.2.4	Mantenimiento de equipos	*Control* Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	*Control* Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	*Control* Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	*Control* Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.
A.11.2.8	Equipos de usuario desatendido	*Control* Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	*Control*

		Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	*Control* Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios	*Control* Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	*Control* Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	*Control* Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2 Protección contra códigos maliciosos		
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
A.12.2.1	Controles contra códigos maliciosos	*Control* Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

A.12.3 Copias de respaldo		
Objetivo: Proteger contra la pérdida de datos.		
A.12.3.1	Respaldo de la información	*Control* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4 Registro y seguimiento		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de eventos	*Control* Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	*Control* Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	*Control* Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	*Control* Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5 Control de software operacional		
Objetivo: Asegurarse de la integridad de los sistemas operacionales.		

A.12.5.1	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6 Gestión de la vulnerabilidad técnica		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	*Control* Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	*Control* Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7 Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		
A.12.7	Controles de auditorías de sistemas de información	*Control* Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13 SEGURIDAD DE LAS COMU NICACIONES		
A.13.1 Gestión de la seguridad de l as redes		
Objetivo: Asegurar la protección de la i nformación en las redes, y sus instalaciones de procesamiento de información de soporte.		
A.13.1.1	Controles de redes	*Control* Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	*Control* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los

		acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	*Control* Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimie de de transferencia información	*Control* Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	*Control* Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	*Control* Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	*Control* Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas		
A.14.1 Requisitos de seguridad de los sistemas de información		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.		

A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	*Control* Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	*Control* La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	*Control* La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.		
A.14.2.1	Política de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	*Control* Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	*Control* Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.

A.14.2.4	Restricciones en los cambios a los paquetes de software	*Control* Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros	*Control* Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	*Control* Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	*Control* La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	*Control* Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	*Control* Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para pruebas.		
A.14.3.1	Protección de datos de prueba	*Control* Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15	**RELACIONES CON LOS PROVEEDORES**	

A.15.1 Seguridad de la información en las relaciones con los proveedores		
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	*Control* Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	*Control* Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	*Control* Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2 Gestión de la prestación de servicios de proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	*Control* Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	*Control* Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.

A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	*Control* Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	*Control* Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	*Control* Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	*Control* El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

A.16.1.7	Recolección de evidencia	*Control* La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**	
A.17.1 Continuidad de seguridad de la información		
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	*Control* La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	*Control* La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		
Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	*Control*

		Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	*Control* *Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización*
A.18.1.2	Derechos de propiedad intelectual	*Control* Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de información de datos personales	*Control* Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
A.18.1.5	Reglamentación de controles criptográficos	*Control*

		Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.		
A.18.2.1	Revisión independiente de la seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	*Control* Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	*Control* Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Fuente: NTC-ISO-IEC 27001:2013

8. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	° Creación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	31/01/2019	01
01	° Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02

9. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: David Yacel Espinosa Vanegas Cargo y/o Vinculación/dependencia: CISO – UNP Contratista - Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Nombre: Mario Alexander Muriel Salamanca Cargo: Coordinador del Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Reviso: Nombre: Samir Manuel Berrio Scaff Cargo y/o Vinculación/dependencia: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Pablo Elías González Monguí Cargo y/o Vinculación/dependencia: Director General	
FIRMA DE OFICIALIZACIÓN DEL PROCEDIMIENTO- SISTEMA DE GESTIÓN	
Oficializó: Nombre: Samir Manuel Berrio Scaff Cargo y/o Vinculación/dependencia: Jefe de la Oficina Asesora de Planeación e Información	