

**EMPRESA MUNICIPAL DE ACUEDUCTO, ALCANTARILLADO
Y ASEO DE FUNZA – EMAAF E.S.P.**

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

**ANGELA MARÍA NERY CÁRDENAS
GERENTE**



Calle 16 No. 16-04 Funza (Cundinamarca)
P.B.X. 822 14 50 FAX: 822 01 67 CEL. 3118875844
e-mail: info@emaafesp.gov.co
C.P. 250020 www.emaafesp.gov.co

INTRODUCCIÓN

La Seguridad de la Información en la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF ESP tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Es por esto que la EMAAF ESP, dentro de su política de gestión del riesgo, vincula acciones para el control de la seguridad de la información y las actividades de valoración de actos inseguros bajo el objetivo de mantener la información de la empresa de manera mucho más confiable, integra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, gestión, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

Integridad: Propiedad que la información se mantenga exacta y completa.

Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVO

Generar acciones frente a la gestión del riesgo bajo enfoque sistemático para una gestión que fortalezca la seguridad de la información en la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF ESP.



ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Empresa que administre sistemas de información a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, tomando como base la guía emitida por el DAFP y los requisitos de la Norma NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de Información.

Metodología de Análisis de Riesgos:

- 1- Identificar los activos de Información de cada proceso
- 2- Identificación de los responsables y dueños de la información(dependencia que produce el activo)
- 3- Identificar: Vulnerabilidades, Amenazas o Causas, Posibles consecuencias, Riesgo (Entrevistas, Observación directa, etc)
- 4- Determinar la probabilidad de ocurrencia para cada riesgo.
- 5- Determinar nivel de valoración del impacto para cada riesgo materializado.
- 6- Determinar el nivel de riesgo basados en la probabilidad de ocurrencia y la valoración del Impacto.

Definiciones:

Factor de Riesgo:

Aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la administración y que afectan de manera directa o indirecta el proceso.



Tipos de Activos:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	Datos importantes o vitales para la Administración de la Entidad: Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustentan la naturaleza legal de la organización o de sus usuarios. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). Datos Clasificados o Calificados: Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos. <u>Ejemplo:</u> Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.



TIPO DE ACTIVOS	DESCRIPCIÓN
Hardware / Infraestructura	Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. <u>Ejemplo:</u> Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Software / Aplicaciones Informáticas	Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. <u>Ejemplo:</u> Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.
Servicios	Funciones que permiten suplir una necesidad de los usuarios (del servicio). <u>Ejemplo:</u> Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico



TIPO DE ACTIVOS	DESCRIPCIÓN
	de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios, Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Soportes de Información	Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo. <u>Ejemplo:</u> Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. <u>Ejemplo:</u> Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	Esenciales para garantizar el funcionamiento de los mecanismos criptográficos. <u>Ejemplo:</u> Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.



TIPO DE ACTIVOS	DESCRIPCIÓN
Equipos Auxiliares	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos. <u>Ejemplo:</u> Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

PROCEDIMIENTO DE DILIGENCIAMIENTO:

Se trata de una hoja Excel. Las primeras cuatro columnas ya están diligenciadas. La cuarta es la descripción del activo al que se le va a evaluar el riesgo-

REGISTRO DE ACTIVOS DE INFORMACIÓN								VALORACIÓN DEL ACTIVO			ANÁLISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD			VALORACIÓN DEL RIESGO INHERENTE DE SEGURIDAD Y		CONTROLES EXISTENTES			
PROPIETARIO/ RESPONSABLE	PROCESO AL QUE PERTENECE	ID	NOMBRE	TIPO (E/F)	DESCRIPCIÓN DEL ACTIVO	MEDIO DE ALMACENAMIENTO	DISPONIBLE PARA CONSULTA	TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	FACTORES DE RIESGO	MANEJO DE RIESGO	CAUSA/AMENAZA	CONSECUENCIA	PROBABILIDAD AD	IMPACTO	TIPIFICACIÓN DEL RIESGO	Descripción de la Actividad o Control Existente
Murkel Rojas	Gestión de Talento Humano	1	Activo	Ambos	Documentos	Disco Duro en el Oficio	SI	Documento	3	3	1	Tecnológicos	Falta de conocimiento al personal	Mala manipulación	Pérdida de tiempo, datos e información	3	3	MODERADO	Capacitación en uso del software

COLUMNA E:

TIPO (E/F): Describe la forma en que está almacenado el activo de información. Es posible diligenciar esta columna con una de las siguientes tres opciones:

- Electrónico
- Físico
- Ambos

COLUMNA G:

MEDIO DE ALMACENAMIENTO: Es con el fin de determinar el lugar donde se está almacenando el activo de información objeto de esta evaluación. Puede ser Discos, CDs, la Nube, En Físico, o una combinación de ellas.

VALORACION DEL ACTIVO:



VALORACIÓN DEL ACTIVO			
TIPO DE ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
Documentos	3	0	1

Se va a realizar en las columnas I a L. Y se va a determinar en orden de importancia cuál de los pilares de la seguridad es más importante para ese activo.

Confidencialidad: Que el contenido de ese activo no sea visto sino únicamente por quien está autorizado para verlo.

Integridad: Que ese activo de información no vaya a ser modificado, sino por las personas autorizadas para tal fin.

Disponibilidad: Que el activo de información esté disponible en el momento y lugar que se necesite.

Criterios de Valoración de Activos:

Criterio	Valor
Alto	4 -5
Medio	2 – 3
Bajo	0 – 1

FACTORES DE RIESGO: Se evaluarán en las columnas N a Q, como se puede ver en la siguiente figura:



Calle 16 No. 16-04 Funza (Cundinamarca)
P.B.X. 822 14 50 FAX: 822 01 67 CEL. 3118875844
 e-mail: info@emaafesp.gov.co
 C.P. 250020 www.emaafesp.gov.co

ANÁLISIS DE RIESGOS RIESGO DE SEGURIDAD Y PRIVACIDAD			
FACTOR DE RIESGO	VULNERABILIDAD / DEBILIDAD	CAUSA / AMENAZA	Consecuencia
Tecnología	Falta de conocimiento el personal	Mala manipulación	Pérdida de tiempo; daño de información

Y los factores de riesgo posibles sobre el activo que se está evaluando pueden ser:

- Personas
- Procesos
- Tecnologías
- Infraestructura
- Factores Externos

Los factores de riesgo corresponden a aquellos agentes que actúan como Disparador de la amenaza

Los factores de riesgo se determinan a partir de:

1. Las vulnerabilidades o debilidades más importantes que puedan llegar a afectar el activo de información que se está evaluando. Ejemplo: Falta de conocimiento del personal.

2. La causa /Amenaza que podría llegar a explotar esa vulnerabilidad. Por ejemplo, la mala manipulación del activo de información.

3. La consecuencia de la explotación de esa vulnerabilidad puede ser en nuestro ejemplo la pérdida de tiempo y el daño en la información. Dentro de las posibles consecuencias podemos enumerar:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad



- Salud y seguridad
- Costo financiero
- Imagen, reputación y buen nombre.

VALORACION DEL RIESGO INHERENTE:

Se va a evaluar en las columnas S a V, como se muestra en la siguiente figura;

VALORACIÓN DEL RIESGO INHERENTE DE SEGURIDAD Y PRIVACIDAD DE LA		
PROBABILIDAD	IMPACTO	TIPIFICACIÓN DEL RIESGO
3	3	MODERADO

Niveles de valoración de **Probabilidad de Ocurrencia**:

NIVEL	CONCEPTO	DESCRIPCIÓN	FRECUENCIA
1	Rara Vez	Puede que no se haya presentado u ocurrir solo en circunstancias excepcionales.	Nunca o no se ha presentado en los últimos 5 años
2	Improbable	Pudo ocurrir en algún momento, es poco común o frecuente	Al menos una vez en los últimos 5 años
3	Posible	Puede ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	Probable	Ocurrirá en la mayoría de las circunstancias.	Al menos una vez en el último año
5	Casi Seguro	Se espera que ocurra en la mayoría de las circunstancias	Más de una vez al año



Niveles de valoración del **Impacto**:

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	Insignificante	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
4	Mayor	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
5	Catastrófico	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.



TIPIFICACION DEL RIESGO:

Se puede determinar mediante la siguiente tabla:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	Mayor o igual a 20	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Mayor o igual a 15 y menor a 20	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Riesgo Moderado	Mayor o igual a 10 y menor a 15	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Menor	Mayor o igual a 5 y menor a 10	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
Riesgo Bajo	Menor a 5 y mayor a 0	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.



Niveles de riesgo validos (Dimensión del riesgo)

CONTROLES EXISTENTES PARA REDUCIR EL RIESGO:

Se trata de establecer si la entidad está ejecutando algún tipo de plan para reducir el impacto del riesgo establecido, en caso de que se llegara a materializar

CONTROLES EXISTENTES
Descripción de la Actividad o Control Existente
Capacitación una vez al año

En el ejemplo de la figura, la actividad descrita es la realización de capacitaciones anuales.

Valoración del Riesgo: (Probabilidad x Impacto)

PROBABILIDAD	5. Casi Seguro				
	4. Probable				
	3. Posible				
	2. Improbable				
	1. Rara vez				
	1. Insignificante	2. Menor	3. Moderado	4. Mayor	5. Catastrófico
	IMPACTO				

Acciones requeridas según el Nivel de riesgo calculado:

Zona de Riesgo Aceptable	Asumir el Riesgo: Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Tolerable	Mitigar el Riesgo: Riesgos que se puede permitir gestionar, que en caso de materialización la entidad se encuentra en la capacidad de asumirlo.
Zona de Riesgo Moderado	Mitigar o Evitar el Riesgo: Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.



Zona de Riesgo Importante	Mitigar o Evitar el Riesgo: Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	Evitar el Riesgo: Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos de conformidad a la gestión de la empresa, por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

- (1) nuevos activos o modificaciones en el valor de los activos,
- (2) nuevas amenazas
- (3) cambios o aparición de nuevas vulnerabilidades
- (4) aumento de las consecuencias o impactos,
- (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición que permitan contextualizar una toma de decisiones de manera oportuna.

CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Se definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización, basado con su criticidad y su valor para el cumplimiento del objeto misional de la EMAAF E.S.P.



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

El presente plan tiene por objetivo comprender e implementar las acciones tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

La definición del marco de seguridad y privacidad de la información y de los sistemas de información en la empresa, define el estado actual del nivel de seguridad y privacidad y las acciones a implementar.

DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P., busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información, basándose en el M.SPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL. Para lo cual cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los riesgos, definiendo y gestionando las respectivas acciones a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.

IMPLEMENTACIÓN

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P., implementa el plan de seguridad y privacidad de la información y de los sistemas de información desarrollando las estrategias de Gestión de riesgos de seguridad y privacidad de la información, buscando proteger los derechos de los usuarios y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información, para lo cual toma como base el MSPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL del cual describe sus directrices en el “Plan de tratamiento de riesgos de seguridad y privacidad de la información vigencia 2021”.

MONITOREO Y MEJORAMIENTO CONTINUO

El plan de seguridad y privacidad de la información, busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información con los que cuenta la EMAAF E.S.P., realizando las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información, para lo cual se toma como



base el M.SPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P. cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad, con el fin de generar los ajustes o cambios pertinentes y oportunos.

De igual forma se revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la información.

PLAN DE ACCIÓN PARA LA VIGENCIA

De acuerdo con el autodiagnóstico realizado en la vigencia 2020, se estiman puntos de priorización en el desarrollo de actividades que permitan avanzar en la fase de implementación del MSPI, contempladas y aprobadas previamente en el marzo de los comités de Gobierno Digital así:

Acciones	Responsable
Inclusión del Oficial de seguridad de la información (artículo 7.1.1. Manual de Políticas de seguridad de la información)	Oficina de planeación-Alta Dirección
Adquirir software licenciado para Sistema de control y seguimiento de dispositivos móviles (7.2. Manual de Políticas de seguridad de la información)	Oficina de planeación-Alta Dirección
Apropiar presupuesto para cumplimiento de Ley 1221 de 2008, cuando se requiera. TELETRABAJO	Oficina de planeación-Alta Dirección
Capacitar acerca de las políticas de seguridad de la información a los funcionarios nuevos y en general anualmente dentro del plan anual de capacitaciones.	Oficina de planeación-Gestión de las TICS - Talento Humano
Implementar control de entrega parcial o total de activos de información por parte de los funcionarios cuando exista desvinculación, vacaciones, incapacidades o licencias.	Oficina de planeación -Gestión de las TICS- Gestión Documental-Talento Humano



Garantizar que la matriz de activos de información se encuentre actualizada y vigente (rol del oficial de la seguridad de la información), cumpliendo con sus principios de confidencialidad, disponibilidad y accesibilidad y según la clasificación y matriz de riesgos de la información (artículo 9.2.2 Manual de Políticas de seguridad de la información)	Oficina de planeación-oficial de la seguridad-gestión documental-funcionarios
Establecer el borrado seguro de información cuando haya desvinculación de funcionarios o reasignación de equipos a nuevas áreas. (oficial de la seguridad de la información y técnico TI)	Oficial de seguridad -Gestión TI
Restringir el uso de medios extraíbles en todos los equipos de cómputo, exceptuando aquellos que por naturaleza de funciones y responsabilidades deba contar con esta opción en cuyo caso se debe dejar constancia. (rol de oficial de la de seguridad y técnico TI)	Oficial de seguridad -Gestión TI
Restringir el uso de llaves de seguridad solamente a funcionarios responsables de uso financiero dentro de la entidad, dejando acuerdos escritos de responsabilidad de su uso.	Oficial de seguridad -Gestión TI
Crear sistemas que permitan limitar el uso de redes autorizadas a funcionarios de distintas áreas, con alertas de intrusión (configurar Directorio activo, en nuevo servidor).	Gestión de las TICS
En términos de política de control de acceso, se debe garantizar la protección y reserva de oficinas con información sensible como CONTRATACIÓN, TALENTO HUMANO, NÓMINA, SST y FINANCIERA, las cuales en la actualidad no cuentan con oficinas cerradas que minimicen el riesgo de ser vulneradas, robo, pérdida, o deterioro físico. Se debe reubicar la caja fuerte de la empresa en un lugar donde no se encuentre tan expuesta.	Oficina de planeación -Alta Dirección
Cumplir y hacer cumplir la política 12 de criptografía, en relación con la transferencia de información, respaldos de datos. (Rol del oficial de la seguridad de la información).	Oficial de la seguridad de la información-Gestión TI-todos los funcionarios



Las áreas consideradas como de acceso restringido (política 12), deben estar monitoreadas con sistema de video permanente y para su ingreso se debe contar con autorización del responsable o jefe de dicha oficina.	Oficina de planeación -Alta Dirección - Subgerencia Administrativa y Financiera
Control y seguimiento de vulnerabilidades mediante hacking ético anual (oficial de seguridad de la información).	Oficina de planeación -oficial de la seguridad de la información
Aplicar la política de escritorio y pantalla limpia	Todos los funcionarios
Hacer uso correcto de las carpetas de respaldos y gestión en las redes de la información	Todos los funcionarios
Informar a Gestión documental, acerca de actualizaciones significativas en los inventarios de activos de información	Todos los funcionarios
Para la eliminación de información pública clasificada y reservada se debe cumplir con el lineamiento de borrado y destrucción seguro (política 13.7)	Oficial de la seguridad de la información- Gestión Documental
Implementar controles de restricción de instalación de software	Gestión TI
Implementar paz y salvo de entrega de información y su ubicación, con la oficina de planeación y el oficial de la seguridad de la información para desvinculación de funcionarios	Oficina de planeación-oficial de la seguridad-gestión documental -talento humano
Cumplir y hacer cumplir política 14 de seguridad en las comunicaciones, garantizando que se haga uso correcto de correos electrónicos de la empresa, que se de uso adecuado a redes sociales y medios masivos de comunicación y que la información se encuentre según su clasificación actualizada, certera, disponible y accesible a clientes internos y partes interesadas, en las plataformas dispuestas para tal fin como la pg web de la entidad en lo relacionado con transparencia de la información.(rol encargado de comunicaciones)	Gestión de comunicaciones



Determinar en plan de comunicaciones cual es el correcto uso del correo electrónico y medios de comunicación masivos de la empresa, y determinar quienes pueden contar con acceso a intranet, correo corporativo y hacer uso de servicios cloud.	Gestión de comunicaciones
Robustecer controles de ciberseguridad implementando segmentación de redes e inclusión de firewall (software y hardware) y hacer seguimiento (oficial de la seguridad de la información y técnico TI)	Oficina de planeación -Gestión de las TICS- Oficial de la seguridad
Dentro del cumplimiento a las políticas de protección de datos personales, se deben colocar avisos que informen sobre el uso de los datos personales a los clientes internos y externos, como información de video de audio, de registro, etc. Y de acuerdo a la norma.	Gestión de comunicaciones
Implementar y promover el cumplimiento de cláusulas de confidencialidad y de propiedad intelectual en los contratos	Oficina de planeación -Talento Humano
Reportar ante el oficial de la seguridad de la información cualquier evento o ataque que se ponga en riesgo la seguridad de la información y a su vez el oficial dará tratamiento y en caso de requerirse dar aviso a las autoridades y entes de control relacionadas, aportando las evidencias del caso.	Oficial de la seguridad -todos los funcionarios
Divulgar el Manual de Políticas, resaltando que el artículo 17.2. , establece que habrá sanciones a quienes debido al incumplimiento de las políticas de seguridad, pongan en riesgo la información de la empresa.	Oficina de planeación -Gestión de Calidad
Implementar Transición IPV4-IPV6 y proyecto adjunto	Oficina de planeación -Alta Dirección - Gestión de las TIC
Definir el plan de continuidad del negocio.	Oficina de planeación -Alta Dirección

