Manual de Políticas
Seguridad y Privacidad de la Información

Alcaldía Municipal de Guadalajara de Buga

ELABORADO POR: Ing. Camilo H. Rojas T. **CARGO:** Profesional Universitario Oficina TIC **FECHA:** Junio 15 de 2020 **Firma**	**REVISADO POR:** Ing. César Andrés Lozano Pulido **CARGO:** Jefe Oficina TIC **FECHA:** Julio 29 de 2020 **Firma**	**APROBADO POR:** Comité Institucional de Gestión y Desempeño - Acta No. 003 de 2020 **CARGO:** Ing. Carlos Humberto Loaiza - Presidente del Comité y Secretario de Planeación Municipal **FECHA:** Agosto 13 de 2020 **Firma**	**ADOPTADO POR:** Dr. Julián Adolfo Rojas Monsalve **CARGO:** Alcalde Municipal de Guadalajara de Buga **FECHA:** Octubre 9 de 2020 **Firma**

Versión	Fecha	Cambios Introducidos
1.0	Junio de 2020	Primera versión del documento

Tabla 1: Control de Versiones

Tabla de Contenido

1 INTRODUCCIÓN **1**

2 OBJETIVO **1**

3 ALCANCE **1**

4 TÉRMINOS Y DEFINICIONES **1**

5 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN **5**

6 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN **6**

6.1 Organización de la Seguridad de la Información 6

6.1.1 Nivel Estratégico 6

6.1.2 Nivel Táctico 7

6.1.3 Nivel Operativo 9

6.2 Recurso Humano 10

6.2.1 Vinculación 11

6.2.2 Ejecución del cargo 11

6.2.3 Desvinculación 11

6.2.4 Personal externo 11

6.3 Gestión de Activos 12

6.3.1 Responsabilidad por los activos de información 12

6.3.2 Identificación de activos 12

6.3.3 Clasificación de la información 13

6.3.4 Etiquetado de la información 13

6.3.5 Gestión de medios removibles 13

6.3.6 Disposición de los activos de información 14

6.3.7 Dispositivos móviles 14

6.4 Control de Acceso 14

6.4.1 Control de acceso con autenticación. 15

6.4.2 Suministro del control de acceso 15

6.4.3 Gestión de contraseñas 15

6.4.4 Perímetros de seguridad 16

6.5 No Repudio 17

6.6 Privacidad y Confidencialidad 17

6.6.1 Tratamiento y protección de datos personales 17

6.6.2 Política de confidencialidad 17
6.6.3 Política de controles criptográficos 18
6.7 Integridad 18
6.8 Políticas de Seguridad para la Adquisición, Desarrollo y mantenimiento de Sistemas 18
6.9 Políticas para Teletrabajo 19
6.10 Disponibilidad del Servicio e Información 20
6.11 Registro y Auditoría 20
6.12 Gestión de Incidentes de Seguridad de la Información 21
6.13 Capacitación y Sensibilización en Seguridad de la información 22
6.14 Políticas Especiales para Terminales de Áreas Financieras 22
6.15 Políticas Adicionales 24
6.15.1 Política de Uso aceptable 24
6.15.2 Política de Escritorio Limpio y Pantalla Limpia 29

1 INTRODUCCIÓN

La información es, tal vez, el activo más importante de cualquier organización. Es por ello que la Administración Municipal de Guadalajara de Buga, siguiendo las directrices trazadas por el Ministerio de Tecnologías de la Información y las Comunicaciones a través de la política de Gobierno Digital (decreto 1008 de 2018), realiza los esfuerzos necesarios para proteger la confidencialidad, la integridad y la disponibilidad de este activo. De esta manera, se garantiza el cumplimiento de los objetivos misionales de la entidad, mejorando la gestión pública y la relación con los ciudadanos.

El presente Manual de Políticas de Seguridad y Privacidad de la información se realiza con base a los lineamientos dados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), mediante la estrategia de Gobierno Digital y, mas específicamente, de los documentos guía «Elaboración de la política general de seguridad y privacidad la información», «Roles y responsabilidades», «Gestión y clasificación de activos de información», «Plan de capacitación y comunicación de seguridad de la información», «Lineamientos: terminales de áreas financieras entidades públicas» y «Cero papel en la Administración Pública». En ocasiones, en el presente manual se harán transcripciones literales de estos documentos, cuando su importancia lo justifique.

2 OBJETIVO

Definir tanto la política general como las políticas específicas que regulan las actividades tanto de empleados como de personal contratista, visitantes y terceros que tienen algún vínculo con la Administración Municipal, y que pretende minimizar los riesgos propios del uso de la información.

3 ALCANCE

Las políticas plasmadas en este documento son de obligatorio cumplimiento tanto para los empleados de todos los niveles jerárquicos y pertenecientes a todos y cada uno de los procesos administrativos y de control de la Alcaldía Municipal de Guadalajara de Buga, como para los contratistas y terceros que tengan algún vínculo con la Administración Municipal. Las políticas también deben ser acatadas por los ciudadanos que hacen uso de los distintos servicios que ofrece la entidad.

4 TÉRMINOS Y DEFINICIONES

Activo de Información. Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo3 . En su sentido más amplio, éstos hacen referencia a la información que se recibe, transforma y produce en la entidad u organismo distrital en el cumplimiento de sus funciones. Tomado de: «*https://secretariageneral.gov.co/sites/default/files/linemientos-distritales/L_11%20Inventario%20de%20Activos%20de%20Informaci%C3%B3n.pdf*».

Acuerdo de Confidencialidad. Es un documento en donde existe el compromiso con otra persona o entidad, de que cierto tipo de información, especialmente la que se ha definido como Clasificada o Reservada y que se va a suministrar a lo largo de una relación comercial, laboral, etc., no será divulgada. Tomado de: «*https://www.misabogados.com/blog/es/*
es-una-clausula-de-confidencialidad».

Acuerdo de Nivel de Servicio (ANS).Un acuerdo de nivel de servicio (service level agreement, SLA) es un contrato entre un proveedor de servicios y sus clientes internos o externos que documenta qué servicios proporcionará el proveedor y define los estándares de servicio que el proveedor está obligado a cumplir.

Tomado de «*https://searchdatacenter.techtarget.com/es/definicion/Acuerdo-de-nivel-de-servicio-o-SLA*»

Amenaza. Según [ISO/IEC 13335-1:2004]: «*Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización*».

Archivo Central. Es el que está conformado por la documentación proveniente de las transferencias recibidas de las distintas oficinas de una entidad.

Archivo de Gestión. Comprende toda la documentación que es sometida a continua utilización y consulta administrativa por las oficinas productoras u otras que la soliciten. Su circulación o trámite se realiza para dar respuesta o solución a los asuntos iniciados.

Autenticación. Es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser.

Autenticación de dos factores.La autenticación en dos factores, también conocida como de doble factor, es un sistema que agrega una capa de seguridad adicional al iniciar sesión con una cuentas en diferentes servicios. No basta solo con una contraseña para iniciar sesión, se pedirá algo más. Al entrar en una cuenta, el sistema pedirá que se confirme la identidad con otro factor diferente. Puede ser mediante un código que se envía a un teléfono por SMS o llamada, el método más común, aunque otros servicios también permiten el uso de otras herramientas como la llave de seguridad o la huella dactilar.

Tomado de : «*https://andro4all.com/2019/04/por-que-utilizar-autenticacion-dos-factores*».

Aviso de Privacidad. El Aviso de Privacidad es el documento físico, electrónico o en cualquier otro formato, puesto a disposición del titular para informarle acerca del tratamiento de sus datos personales. A través de este documento se comunica al titular la información relacionada con la existencia de las políticas de tratamiento de información de una entidad y que le serán aplicables, la forma de acceder a las mismas y las características del tratamiento que se pretende dar a los datos personales.

Borrado Seguro. Es un método de eliminación de información almacenado en un medio que no permite la recuperación posterior de la misma.

Centro de Procesamiento de Datos (CPD). Se denomina así al espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Cifrado. En el mundo de la informática, el cifrado es la conversión de datos de un formato legible a un formato codificado, utilizando métodos matemáticos, y que solo se pueden leer o procesar después de haberlos descifrado.

Clasificación de Activos de Información. Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

Cláusula de Confidencialidad. Las cláusulas de confidencialidad son disposiciones particulares dentro de un contrato por el cual el empleador impone la obligación al trabajador de mantener reserva de cierto tipo de información que es considerada de vital importancia para la empresa. El incumplimiento de este pacto de confidencialidad puede traer sanciones que en la misma cláusula o contrato se tipifican.

Código Malicioso. Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos y spyware.

Tomado de «*http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/28*».

Comité de Seguridad de la Información. Son responsables de entregar las directrices para conformar el Manual de Políticas de Seguridad de la Información de la entidad, tramitar recursos para administrar los incidentes de seguridad u otras vulnerabilidades o riesgos, velar por el cumplimiento de las políticas, normas y

procedimientos derivados de la misma, como también de fomentar planes de difusión, capacitación y formación de la cultura de seguridad de la información.

Conexión Remota. Es una tecnología que permite acceder a determinados recursos de un sistema informático desde una terminal situada por fuera de sus límites y utilizando, generalmente, redes públicas como Internet.

Confidencialidad. Propiedad que garantiza que la información no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria.

Cookies. Es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del navegador.

Credenciales de Acceso. Las credenciales son los elementos de que dispone un sujeto o sistema para comprobar su identidad y obtener el acceso a ciertos recursos.

Custodio de la información. Son los individuos o grupos que proveen un alto nivel de confianza y a los cuales se les deja en posesión y responsabilidad, delegada por su dueño, de velar por la seguridad de información que no les pertenece. Se compara con el dueño de los datos. Este rol es ejecutado, normalmente, por personal de la Gerencia de Sistemas, para la información digital. Entre sus deberes están los respaldos y sus verificaciones, la recuperación de información desde dichos respaldos y mantener los registros con los resguardos asociados a su nivel de clasificación. Los custodios de información física son responsables de protegerla y resguardarla de accesos indebidos o no autorizados.

Disponibilidad. Propiedad que garantiza que la información es accesible en el momento en que los usuarios autorizados (personas, organizaciones o procesos) tienen necesidad de acceder a ella.

Gabinete de Comunicación. Es un armario donde se instalan equipos de comunicación que permiten la distribución de una conexión principal en varias conexiones de punto final.

Gestión de Cambios. El objetivo primordial de la Gestión de Cambios es que se realicen e implementen adecuadamente todos los cambios necesarios en la infraestructura y recursos TI, garantizando un mínimo de interrupciones en la prestación de servicios de TI.

Incidente de Seguridad. Un Incidente de Seguridad de la Información es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

Tomado d*e https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/publicaciones/que-es-un-incidente*».

Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014.

Información pública reservada: Es aquella información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.

Integridad. Propiedad que garantiza que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento.

Llave de Seguridad. Es un dispositivo que se conecta a un puerto USB, y que funciona como método de autenticación.

Medio Removible. Son todos aquellos dispositivos electrónicos que almacenan información y pueden ser conectados y removidos fácilmente del equipo de cómputo.

No Repudio. El no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

Tomado de «*https://glosarios.servidor-alicante.com/ciberseguridad/no-repudio*».

Perímetro de Seguridad física. Son áreas perfectamente delimitadas y que requieren un mayor nivel de seguridad para proteger los activos de información más sensibles para una organización.

Perfil de Acceso. Un perfil de acceso, o perfil de usuario, se define como los permisos y acciones que podrá realizar un usuario determinado en un sistema. Algo así como los «privilegios» que tendrá un usuario en particular.

Tomado de «*http://help.imagestion.cl/5/pages/show/244*».

Plan de Continuidad del Negocio.Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Tomado de «*https://es.wikipedia.org/wiki/Plan_de_continuidad_del_negocio*».

Plan de Recuperación de Desastres. Es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

Tomado de «*https://es.wikipedia.org/wiki/Plan_de_recuperación_ante_desastres*».

Política. Se puede definir como el conjunto de lineamientos generales que orientan un proceso y que facilitan la toma de decisiones.

Portal Cautivo. Es una página de inicio de sesión personalizado en redes empresariales que los usuarios invitados deben pasar antes de poder conectarse a la red Wi-Fi.

Tomado de «*https://www.linksys.com/es/r/resource-center/portal-cautivo/*».

Propietario o Dueño de la información. Es el individuo o grupo de individuos responsable de ciertos datos específicos. Son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Pruebas de Vulnerabilidad. Es una técnica utilizada por profesionales de seguridad de la información para encontrar y corregir fallas de seguridad en los activos de información.

Reconocimiento Biométrico. Son sistemas que permiten el reconocimiento de personas mediante la medición de alguno de sus rasgos biológicos (biometría), como por ejemplo, la huella dactilar, el iris, la cara, la forma de la mano, la voz, etc.

Riesgo de Seguridad. Es la probabilidad de que se materialice una amenaza de seguridad sobre un activo de información, explotando alguna vulnerabilidad del mismo.

Segregación de Ambientes. En el desarrollo de Software, se refiere técnicas que permiten aislar cambios y desarrollos en período de prueba, antes de ser trasladados a producción.

Seguridad Física. Son las acciones que permiten minimizar los riesgos de daños y accesos físicos no autorizados a la información y a las operaciones de una organización mediante el establecimiento de perímetros de seguridad y áreas protegidas.

Seguridad Lógica. La seguridad lógica garantiza la seguridad a nivel de los datos, permitiendo el acceso lógico a la información sólo a personas autorizadas.

Sensibilización. Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

Sistema de Alimentación Ininterrumpida (UPS). Es un dispositivo que, gracias a sus baterías u otros elementos que almacenan energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

Tomado de «*https://es.wikipedia.org/wiki/Sistema_de_alimentación_ininterrumpida*».

SPAM. Spam, o información basura, hace referencia a aquellos mensajes, con remitente desconocido, que no son solicitados ni deseados por el usuario y que, además, por norma general, son enviados en grandes cantidades. Por consiguiente, el spam se caracteriza por ser anónimo, masivo y no demandado.

Tomado de «*http://www.valortop.com/blog/que-significa-spam*».

Suplantación de Identidad. Es hacerse pasar por un usuario autorizado, disfrutando de los privilegios de este para, con un fin en especial, poder acceder a recursos o sistemas informáticos.

Teletrabajo. Teletrabajo es el término bajo el cual se conoce el esquema acordado formalmente entre un empleado y su empleador para trabajar en un lugar diferente a la oficina. El aprovechamiento de las ventajas de las Tecnologías de información y comunicación permite lograr las actividades en forma no presencial, trayendo consigo la ventaja de evitar pérdidas de tiempo en desplazamiento y poder trabajar desde la comodidad de su lugar de vivienda. Tomado de «*https://www.ssf.gov.co/documents/20127/143673/Pol%C3%ADtica+de+teletrabajo.docx/b930fd2d-24ce-3a26-c749-e949d1b95d1d*».

Titular de Datos Personales. Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos. Ejemplo: Un usuario que celebra un contrato de prestación de servicio.

Token. Es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Uso eficiente del Papel. Es la reducción continúa y ordenada en el uso del papel que requiere la entidad, mediante la sustitución de los documentos físicos por medios electrónicos. Es un aporte de la administración electrónica que se refleja en la creación, gestión y almacenamiento de documentos de archivo en soportes electrónicos, gracias a la utilización de Tecnologías de la Información y las Comunicaciones.

Usuario. es cualquier persona autorizada que interactúe con el sistema y sus datos. Son considerados los consumidores de la información y deben velar por la preservación de la clasificación de la información en su uso cotidiano. Para la información física etiquetada como Restringida o Confidencial, debe protegerla del libre acceso y entregarla al dueño o responsable de ésta. Es responsabilidad de cada usuario proteger y resguardar toda información confidencial o restringida.

5 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Administración Municipal de Guadalajara de Buga con respecto a la protección de los activos de información, que aportan valor para promover una ciudad para todos, incluyente y de crecimiento sostenible, de participación ciudadana, convivencia y transparencia; mejorando las condiciones de productividad y competitividad para el desarrollo económico, turístico y social, manteniendo la preservación de su memoria y su identidad cultural. Por ello, implementa, mantiene y mejora el Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Alcaldía Municipal de Guadalajara de Buga en cumplimiento de la política, establece los siguientes objetivos:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Implementar y mantener la eficacia del Modelo de Seguridad y Privacidad de la Información implementado en la entidad.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del la Alcaldía Municipal de Guadalajara de Buga
- Garantizar la continuidad de la seguridad de la información frente a los incidentes que puedan afectar la continuidad del negocio.

6 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Organización de la Seguridad de la Información

La Administración Municipal definirá y establecerá los roles y responsabilidades necesarios para la implementación del Modelo de Seguridad y privacidad de la Información (MSPI). Estos roles y responsabilidades estarán enmarcadas bajo los niveles estratégico, táctico y operativo.

6.1.1 Nivel Estratégico

La Administración Municipal conformará formalmente el **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN** como la instancia interna que orientará la implementación y el mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI). El comité estará integrado, entre otros perfiles, por los siguientes:

- El Alcalde Municipal o a quién él delegue formalmente.
- El Secretario de Planeación Municipal o su representante (Planeación y Gestión de Calidad)
- El Secretario de Desarrollo Institucional o su delegado (Recurso Humano y Gestión Documental)
- El Jefe de la Oficina Jurídica o su delegado
- El Jefe de la Oficina TIC o su delegado
- El Jefe de Control Interno Administrativo o su delegado
- El responsable de la seguridad de la información

Este comité, además de formular las políticas descritas en el presente documento y verificar el cumplimiento de las mismas, tendrá como objetivo el asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad y privacidad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo. Igualmente, son funciones de este comité:

1. Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la entidad.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información, en especial al RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN y al RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y, según los resultados de esta revisión, definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

Las funciones del Comité de Seguridad de la información podrán ser asumidas por el Comité Institucional de Gestión y Desempeño.

6.1.2 Nivel Táctico

La Administración Municipal definirá, a este nivel, al **PROFESIONAL DE LA SEGURIDAD DE LA INFORMACIÓN** quien será el líder del proyecto y del equipo de gestión al interior de la entidad, y que también tendrá las siguientes responsabilidades específicas, de acuerdo a temas como Servicios Tecnológicos, Estrategia TI, Gobierno TI, Sistemas de Información, Información y Uso y Apropiación:

DOMINIO	RESPONSABILIDADES
Servicios Tecnológicos	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. • Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
Estrategia TI	• Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
Gobierno TI	• Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la dinamización de los riesgos del componente de TI. Encargado de monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.

Sistemas de Información	• Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. • Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. • Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
Información	• Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
Uso y Apropiación	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

6.1.3 Nivel Operativo

La Administración Municipal debe conformar un **EQUIPO DEL PROYECTO** al cual deben pertenecer miembros directivos y/o representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la Oficina TIC. Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

De acuerdo a la composición orgánica de la Entidad, se proponen los miembros del equipo de seguridad y privacidad de la información, de acuerdo a los siguientes perfiles:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área Jurídica.
- Responsables y/o encargados del Tratamiento de Datos Personales

Responsabilidades del equipo del proyecto:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

Además de las responsabilidades anteriormente citadas, los responsables y/o encargados del tratamiento de datos personales tendrán los siguientes deberes:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

6.2 Recurso Humano

La Secretaría de Desarrollo Institucional o, en su defecto, la dependencia o área que realiza la vinculación de personal a la Entidad, debe realizar las siguientes actividades que van orientadas a mantener la seguridad de la información. Igualmente, la Administración Municipal llevará a cabo las acciones necesarias para garantizar la correcta gestión de los activos de información por parte de empleados y contratistas, activando los procesos administrativos o disciplinarios necesarios cuando se incumplan las Políticas de Seguridad de la Información. La alta dirección de la entidad debe mostrar su compromiso con la seguridad de la información por medio de la aprobación y apoyo a la implantación del presente manual de políticas.

6.2.1 Vinculación

- Realizar la verificación de la información contenida en la hoja de vida del solicitante antes de formalizar su vinculación a la Entidad.
- Verificar los antecedentes de todos los candidatos a un empleo de planta o por contrato, de acuerdo a la clasificación de información a la que va a tener acceso y de acuerdo a los riesgos que se perciban y que puedan afectar la seguridad de la información.
- Certificar que los funcionarios a vincular firman en calidad de aceptación el conocimiento de la políticas de seguridad contenidas en el presente manual y un acuerdo o cláusula de confidencialidad. Estos documentos serán anexados a los demás proporcionados por el nuevo funcionario.

6.2.2 Ejecución del cargo

- La Administración Municipal implementará programas de sensibilización en seguridad de la información para todo el personal y proveerá los recursos para llevarlos a cabo. Esto con el fin de promover el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
- La Secretaría de Desarrollo Institucional en conjunto con la Oficina TIC serán los encargados de convocar a empleados, contratistas y terceros, al menos una vez al año, a eventos programados para sensibilizar en temas de seguridad de la información.
- Los empleados, contratistas y terceros del Municipio deben dar cumplimiento a lo estipulado en este manual de políticas de seguridad de la información y deben asistir a los eventos a los que sean convocados bajo el programa de se sensibilización.
- Tanto empleados como contratistas del Municipio deben ser cuidadosos de no divulgar información etiquetada como CLASIFICADA o RESERVADA sin la previa autorización de su propietario.
- El incumplimiento al presente manual de políticas acarreará la interposición de sanciones correspondientes, contempladas en el Código Único Disciplinario y normas aplicables concordantes.

6.2.3 Desvinculación

- Al momento de su desvinculación o cambio de cargo o funciones, los empleados o contratistas de la Alcaldía Municipal de Guadalajara de Buga deben hacer entrega formal de los activos de información que se encontraban a su cargo de acuerdo al procedimiento que se tenga para tal fin. En el caso del personal contratista, esto deberá ser verificado por el supervisor del contrato.
- La Secretaría de Desarrollo Institucional o cada Secretario de Despacho o Jefe de Oficina deberá reportar lo antes posible a Oficina TIC y demás oficinas interesadas, la desvinculación o cambio de cargo o labores de los funcionarios o personal provisto por terceras partes, para que se lleven a cabo los cambios y ajustes necesarios en materia de seguridad de la información.

6.2.4 Personal externo

- Certificar que el personal provisto por terceros que, en razón de sus funciones, tenga acceso a la información de la Alcaldía Municipal de Guadalajara de Buga, firmen en calidad de aceptación el conocimiento de las políticas de seguridad y un acuerdo o cláusula de confidencialidad antes de otorgar acceso a las instalaciones o a alguna plataforma tecnológica.

6.3 Gestión de Activos

La Administración Municipal proporciona a empleados, contratistas y terceros autorizados, una serie de activos de información (archivos físicos, información, equipos, sistemas y servicios), para llevar a cabo las actividades propias de su función, permitiendo cumplir los objetivos de la entidad. Estos activos son y seguirán siendo de propiedad del Municipio de Guadalajara de Buga, deben ser inventariados, clasificados y se debe asignar un responsable a cada uno de ellos.

6.3.1 Responsabilidad por los activos de información

- Cada Secretario de Despacho o Jefe de oficina debe actuar como responsable de los activos de información de la dependencia a su cargo, lo que le da la facultad para aprobar o revocar el acceso a su información tanto física como electrónica. Igualmente, y en coordinación con la Oficina TIC, debe mantener un inventario actualizado de dichos activos teniendo en cuenta la Guía para la Gestión y Clasificación de Activos de Información.
- La Oficina de Tecnologías de la Información y las Comunicaciones (TIC) es responsable tanto de los activos de información en su área, como de los activos de información que soportan los distintos sistemas de información y las comunicaciones de la entidad.
- Los responsables por los activos de información deben monitorear de forma periódica la validez de los usuarios y de sus perfiles de acceso.
- Los usuarios de los diferentes activos de información deben utilizar estos recursos sólo para las funciones propias de su cargo. No deben ser utilizados para fines diferentes a estos, como el almacenamiento de archivos multimedia personales (fotos, video, música, etc.).
- No se permitirá conectar a la red interna equipos de cómputo ajenos a los proporcionados por la Administración Municipal, a menos que esto pueda hacerse bajo condiciones de seguridad suficientes que permitan aislarlos de tal forma que no se pueda acceder desde ellos a información no autorizada.
- Si le logran proporcionar las condiciones de seguridad suficientes que permitan, por ejemplo, aislmaiento mediten VLAN, autenticación mediante portal cautivo, etc. y se necesitase conectar un equipo personal a la red de la entidad, se deberá solicitar autorización previa a la Oficina TIC en donde se valorará si el equipo de cómputo cumple con ciertos niveles mínimos de seguridad y con la legalidad del software instalado.

6.3.2 Identificación de activos

- Es competencia del responsable elaborar y actualizar el inventario de sus activos de información con una frecuencia de, al menos, dos veces al año, en coordinación con la Oficina TIC y utilizando las herramientas e instrumentos que estos dispongan.
- La herramienta utilizada para mantener el inventario de activos de información debe permitir la identificación única de cada activo y su propietario.
- El inventario de Activos de Información debe hacerse conforme a las directrices de la Guía No. 5 (Guía para la Gestión y Clasificación de Activos de Información) publicada por MINTIC.

6.3.3 Clasificación de la información

- La Alcaldía Municipal de Guadalajara de Buga a través del Comité de Seguridad y Privacidad de la información, o quien haga sus veces, definirá los niveles más adecuados para clasificar su información (física y electrónica), de acuerdo a la criticidad, sensibilidad y reserva de la misma. Esto debe hacerse teniendo en cuenta las leyes y normativas que en el momento afecten a la entidad, como por ejemplo, la Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, Decreto 1081 de 2015, entre otras, y buscando dar cumplimiento a los requerimientos estipulados en el ítem relacionado con la Gestión de Activos de los estándares 27001:2013, ISO 27002 e ISO 27005.
- Del proceso anterior saldrá un guía de clasificación que permita a los responsables catalogar su información y establecer los controles técnicos y administrativos necesarios para garantizar su confidencialidad, integridad y disponibilidad. La aplicación de la guía de clasificación deberá ser monitoreada periódicamente.
- Todos los funcionarios de la Administración Municipal deben conocer y cumplir con los lineamientos establecidos en la guía de clasificación, para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información tanto física como electrónica.
- Se deben seguir las recomendaciones en cuanto al esquema de clasificación publicados en la Guía para la Gestión y Clasificación de Activos de Información de MINTIC, para cada una de las propiedades de confidencialidad, integridad y disponibilidad.

6.3.4 Etiquetado de la información

- Toda la información que esté clasificada según el esquema adoptado deberá etiquetarse de tal manera que indique los niveles de clasificación en relación a las propiedades de confidencialidad, integridad y disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (confidencialidad, integridad y disponibilidad) como NO CLASIFICADO, lo que implica que deben ser tratados como activos de **información pública reservada**, de **integridad alta** y de **disponibilidad alta**.
- Para el etiquetado, deben adoptarse las recomendaciones de la Guía No. 5 (Guía para la Gestión y Clasificación de Activos de Información) del MINTIC.

6.3.5 Gestión de medios removibles

Teniendo en cuenta el riesgo potencial a la seguridad derivado del uso de medios removibles y que tiene que ver tanto con la propagación de código malicioso como con la extracción no autorizada de información confidencial, la Administración Municipal debe establecer los controles necesario que minimicen estas posibilidades.

- Se restringirá el uso de dispositivos de almacenamiento removibles en los equipos de cómputo de la Administración Municipal.
- Las autorizaciones para habilitar el uso de dispositivos removibles debe tramitarse a través del Comité de Seguridad y Privacidad de la Información, o quien haga sus veces, quienes determinarán, de acuerdo a un análisis de riesgos y a la clasificación de la información almacenada en el equipo de cómputo, si es posible llevarla a cabo.
- Los responsables de los equipos de cómputo a quienes se otorgue autorización para el uso de medios extraíbles, son responsables también del mal uso que se pueda dar a estos dispositivos.
- La solución antivirus de todos los equipos de la Administración Municipal deberá tener activo tanto el escaneo automático de virus para los medios removibles como el bloqueo de la reproducción automática de archivos ejecutables.

6.3.6 Disposición de los activos de información

La Administración Municipal de Guadalajara de Buga deberá diseñar un procedimiento, y velar por su cumplimiento, mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o re uso de los activos de información cuando estos ya no se requieran y teniendo en cuenta los siguientes aspectos:

- Se deberá hacer una copia de seguridad de la información importante contenida en los activos de información (medios de almacenamiento fijos y removibles) objeto de la eliminación, retiro, traslado o re uso, las cual deberá ser etiquetada debidamente y almacenada por un tiempo establecido previamente en el procedimiento.
- Si se decide eliminar la información contenida en algún medio de almacenamiento fijo o removible, este proceso deberá realizarse con métodos que permitan el borrado seguro y sin marcha atrás, para preservar la confidencialidad.
- La ejecución del procedimiento deberá ser autorizada tanto por el propietario o dueño del activo de información como por su custodio.

6.3.7 Dispositivos móviles

Debido a que la entidad no puede ejercer control sobre los dispositivos móviles ajenos, únicamente se autoriza la conexión de esta clase de dispositivos a las redes de la Administración Municipal cuando sean de propiedad de la Alcaldía Municipal de Guadalajara de Buga, y teniendo en cuenta lo siguiente:

- Los dispositivos móviles de la Administración Municipal sólo deben ser utilizados para tareas propias de la labor que desempeña el funcionario.
- Para que estos equipos puedan utilizarse tanto en la red interna como en otras redes, deberá implementarse en ellos los controles de seguridad necesarios para evitar afectaciones a la confidencialidad, integridad y disponibilidad:
  - Los dispositivos móviles de la Administración Municipal no deben dejarse desatendidos en lugares públicos. En viajes, deben llevarse como equipaje de mano.
  - Se deben implementar métodos que garanticen un control de acceso al dispositivo, como por ejemplo contraseñas fuertes o acceso mediante información biométrica. Igualmente, y como protección adicional, podrían utilizarse métodos de cifrado que mantengan oculta la información ante accesos no autorizados.
  - Los elementos tecnológicos móviles deben mantener siempre su software antivirus activado y actualizado, al igual que su cortafuegos.
  - Se debe evitar conectar los equipos móviles a redes abiertas o de dudosa procedencia.
- Los equipos móviles, al ser propiedad de la Alcaldía Municipal, pueden ser solicitados o inspeccionados por parte de personal autorizado de la Administración Municipal para fines de control de inventario o de temas de seguridad.
- Los dispositivos móviles deben ser devueltos a la Administración Municipal cuando cese la actividad para la que fue asignada o cese la relación laboral del responsable del elemento tecnológico.

6.4 Control de Acceso

La Alcaldía Municipal de Guadalajara de Buga debe establecer los métodos necesarios para controlar el acceso, tanto físico como electrónico, a la información de la Entidad.

6.4.1 Control de acceso con autenticación.

Para el acceso tanto a las redes como a las aplicaciones y los sistemas de información, la Administración Municipal deberá definir los procedimientos necesarios que permitan autenticar, autorizar y auditar a los diferentes usuarios que requieran de estos servicios. Deben tenerse en cuenta los siguientes aspectos:

- Se debe restringir el acceso a las redes de datos, las aplicaciones y los sistemas de información sólo a aquellos funcionarios y contratistas de la Administración Municipal que necesiten estos servicios para ejercer su labor y sólo desde equipos de cómputo o dispositivos móviles de propiedad de la Alcaldía Municipal, salvo las excepciones que determine el Comité de Seguridad y Privacidad de la Información.
- El acceso a terceros se dará sólo cuando se pueda garantizar un aislamiento seguro de tipo lógico o físico de estos con la red de la Entidad y se debe garantizar también su identificación y control mediante, por ejemplo, sistemas de portal cautivo.
- El acceso a redes de datos, aplicaciones o sistemas de información debe hacerse a través de métodos que permitan identificar al usuario (autenticación), a través mecanismos como el uso de contraseñas, la utilización de alguna característica biométrica (huella dactilar, reconocimiento de retina, facial o de voz, etc) o el uso de elementos que posea el funcionario para su identificación (tarjetas inteligentes, tokens, etc.). En el caso de acceso a recursos sensibles, este debería hacerse a través de autenticación de dos factores.
- La Oficina TIC será la encargada de gestionar los usuarios en redes, aplicaciones y sistemas de información. Igualmente, será quien indique los lineamientos o procedimientos a tenerse en cuenta para la creación, modificación, bloqueo o eliminación de las cuentas de usuario, con las autorizaciones respectivas por parte de los líderes de las distintas dependencias de la Entidad.
- Los diferentes usuario de los servicios ofrecidos por la entidad deben tener claro que, independientemente del método de autenticación utilizado, este es personal e intransferible y no debe prestarse ni compartirse. El titular se hace responsable por una mala utilización del mismo.

6.4.2 Suministro del control de acceso

Se deben construir los procedimientos y directrices necesarias para gestionar la asignación, modificación, revisión o revocación de derechos y/o privilegios a los usuarios. En principio, tomar en cuenta lo siguiente:

- Las solicitudes de creación, modificación, revisión o revocación de cuentas y privilegios debe hacerse mediando una autorización por parte del líder de la dependencia a que pertenezca el usuario. En esta solicitud debe indicarse, además de los datos personales y de identificación del usuario, los recursos a que debe tener acceso y los privilegios que se pretenden obtener en ellos.
- La autorización para la gestión de los usuario especiales, como administradores de infraestructura, aplicaciones y sistemas de información, debe hacerse mediante el Comité de Seguridad y Privacidad de la Información.
- La gestión técnica de privilegios de usuario debe estar a cargo de la Oficina TIC de la entidad.

6.4.3 Gestión de contraseñas

- La entidad debe establecer los requisitos de calidad mínimos que deben tener las contraseña utilizadas por los diferentes usuarios, para que estas sean consideradas como fuertes y que no comprometan la seguridad de las redes, las aplicaciones y los sistemas de información. Deben tenerse en cuenta los siguientes requisitos mínimos:

  - La contraseña debe constar de, al menos, ocho (8) caracteres.
  - La contraseña debe tener una combinación de, al menos, tres de los siguientes elementos:
    * Letras en mayúsculas
    * Letras en minúscula
    * Números
    * Caracteres especiales
  - No debe usarse información personal del usuario en las contraseñas como nombres y fechas.
- La solicitud de nuevas contraseñas o las que resulten del reinicio de estas, cuando la plataforma no permita hacerla de forma directa, deberán hacerse de forma personal y por escrito. La nueva contraseña deberá ser enviada directamente al usuario a través de un medio seguro y se obligará al usuario a que la cambie inmediatamente tras el primer ingreso.
- Debe obligarse al usuario a cambiar su contraseña al menos cada seis (6) meses.
- La contraseña no debería estar escrita en medios poco seguros.

6.4.4 Perímetros de seguridad

La entidad debe tener siempre bien definidas las áreas de seguridad en donde se encuentre información crítica o se realice el almacenamiento o procesamiento electrónico de la misma. Inicialmente, se reconocen la siguientes áreas de seguridad en la Alcaldía Municipal de Guadalajara de Buga:

- Centro de procesamiento de datos (CPD). Ubicado en el tercer piso del Centro Administrativo Municipal de Buga (CAMB).
- Gabinetes de comunicaciones. Ubicados en el segundo y primer piso del CAMB, y dos (2) más en el edificio antiguo, para un total de cuatro (4) gabinetes de comunicaciones.
- Archivo central de la Alcaldía Municipal. Localizado en dos ubicaciones: edificio antiguo e instalaciones de los «Talleres Municipales».
- Archivos de Gestión en cada dependencia de la Administración Municipal.

La Administración Municipal debe garantizar la seguridad del perímetro donde se encuentran estas áreas de seguridad, controlando las amenazas internas y externas y las condiciones medioambientales. Debe cubrirse, como mínimo, los siguientes aspectos:

- Sistema de alimentación ininterrumpida (UPS), si aplica.
- Sistema de control de temperatura y humedad
- Sistema de control de incendio
- Sistema de vigilancia y monitoreo

Igualmente, se deben convertir en áreas de acceso restringido, en donde sólo se permita el acceso a los líderes de las dependencias responsables y a los funcionarios que por la naturaleza de su trabajo deban ingresar a estos perímetros. Los terceros que deban realizar alguna labor eventual deberán gestionar antes un permiso temporal con los líderes y, si este es otorgado, deben permanecer acompañados por un funcionario autorizado mientras ejerzan la labor.

Los ingresos y salidas a estas áreas deben ser debidamente registrados para llevar la trazabilidad de quién ingresa a éstas, qué labores desarrolla, firma y fecha y hora tanto de ingreso como de salida.

6.5 No Repudio

La Administración Municipal debe implementar mecanismos que eviten que los usuarios nieguen haber realizado alguna acción sobre los activos de información. Para llevar a cabo esta implementación, debe tenerse en cuenta:

- **La trazabilidad**. Se debe registrar cada acción que se realice sobre un activo de información y que permita conocer quién crea información, quién origina y quién recepciona una comunicación de información y quién entrega información, entre otras.
- **La retención**. Se debe indicar claramente por cuánto tiempo se mantendrán los registros de trazabilidad. En sistemas de información o aplicaciones importantes se debe mantener los registros almacenados por al menos dos años.
- **La Auditoría**. Se deben realizar auditorías continuas a los mecanismos implementados para asegurarse que se están registrando adecuadamente las acciones sobre los activos de información y tomar los correctivos necesarios.
- **Intercambio electrónico de información**. Cuando se tengan implementados procesos de intercambio electrónico de información, como por ejemplo trámites o servicios en línea u otros, la entidad debe asegurarse que se usan los instrumentos necesarios para controlar el no repudio.

6.6 Privacidad y Confidencialidad

6.6.1 Tratamiento y protección de datos personales

Los pormenores sobre el tratamiento y protección de datos personales por parte de la Alcaldía Municipal de Guadalajara de Buga está plasmado en el documento «Políticas Tratamiento de Datos Personales», aprobado mediante Resolución DAM-1100-057-2019 y que puede obtenerse en el enlace http://www.guadalajaradebuga-valle.gov.co/politicas-y-lineamientos/politica-de-tratamiento-y-proteccion-de-datos-personales.

6.6.2 Política de confidencialidad

La Administración Municipal de Guadalajara de Buga hará firmar un acuerdo de confidencialidad a los empleados, contratistas, practicantes, terceros y, en general, a todos aquellos que hayan obtenido autorización para acceder a la información de la entidad. Este acuerdo podrá ser una cláusula de confidencialidad que sea parte integral del contrato para contratistas, practicantes o terceros. El acuerdo o cláusula debe abarcar lo siguiente:

- Debe contener un compromiso de no divulgar información interna y externa que el funcionario, contratista o tercero conozca de la entidad, así como las funciones que este desempeña en la misma.
- Implica que la información conocida por todo funcionario, contratista o tercero bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con autorización previa.
- El acuerdo o la cláusula contendrá las responsabilidades y las consecuencias que podría tener el incumplimiento de la misma.
- El acuerdo o cláusula de confidencialidad deberá tener vigencia desde el momento de la firma del acuerdo o del contrato que contiene la cláusula hasta, como mínimo, un año después de terminar la vinculación con la entidad.

6.6.3 Política de controles criptográficos

Se debe proteger la información sensible de la Administración Municipal de acuerdo a su clasificación y a través de técnicas criptográfica que permitan garantizar su confidencialidad e integridad tanto en su almacenamiento como en su transmisión y transporte.

- La Oficina de Tecnologías de la Información y las Comunicaciones serán los encargados de definir las técnicas de cifrado que se deberán usar tanto para el almacenamiento de información clasificada y reservada como para la comunicación y el transporte de ésta, lo cual se hará teniendo en cuenta en análisis de riesgos, las disposiciones legales y considerando criterios de confidencialidad, integridad, autenticidad y no repudio. Deberá preferirse el uso de las técnicas de cifrado más avanzadas que existan en cada momento, lo que garantizará la mejor protección.
- La información sensible que se almacene de forma local, deberá usar técnicas de cifrado que permita mantenerla de forma segura, inclusive si el medio de almacenamiento llega a manos no autorizadas.
- La comunicaciones, en especial las que se hacen a través de redes públicas como Internet, serán protegidas con protocolos de cifrado que permitan establecer comunicaciones seguras.
- La comunicaciones inalámbricas serán protegidas con los protocolos de cifrado más avanzados hasta le momento para este fin y se utilizarán claves fuertes como llave de cifrado.
- Se deberán utilizar técnicas de cifrado para el almacenamiento de información sensible que se transporte en medios removibles, como discos duros externos, memorias USB o SD/MicroSD, etc.
- La gestión de las claves de cifrado será tarea del responsable de la información y contará con el apoyo técnico del personal de TI. Esta gestión de claves debe la generación u obtención de claves, distribución de claves a usuarios, almacenamiento de claves, cambios y actualizaciones de las mismas, revocación de claves (desactivación o retiro), recuperación de claves en caso de pérdidas, etc.

6.7 Integridad

La política de integridad es un compromiso de los funcionarios, contratistas y terceros para que toda información verbal, física o electrónica deba ser adoptada, procesada y entregada o transmitida de forma integral y coherente, exclusivamente a las personas correspondientes y a través de los medios adecuados, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

- La política de integridad deberá ser conocida y aceptada por cada funcionario, contratista y/o tercero de la entidad que conozca o administre información de la entidad.
- En el caso de una vinculación contractual, el compromiso de administración y manejo íntegro e integral de la información interna y externa hará parte de las cláusulas del mismo contrato, bajo la denominación «cláusula de integridad de la información».
- La vigencia del compromiso de mantener la integridad de la información deberá empezar en el momento en que inicie la vinculación del personal e irá hasta, mínimo, un año después de culminar dicha vinculación.

6.8 Políticas de Seguridad para la Adquisición, Desarrollo y mantenimiento de Sistemas

La Oficina TIC establecerá las disposiciones necesarias para garantizar que el desarrollo, tanto interno como externo, de los sistemas de información destinados a la Administración Municipal, se hagan bajo los controles de seguridad adecuados para garantizar la protección de la información de la entidad. Para esto, se deben tener en cuenta las siguientes disposiciones:

- La Oficina de Tecnologías de la Información y las Comunicaciones es la única dependencia con la idoneidad y la capacidad para adquirir, desarrollar e implementar soluciones tecnológicas en la Administración Municipal y para avalar la adquisición y recepción de software de cualquier índole en el marco de convenios y contratos con terceros, conforme a los requerimiento de las demás dependencias y con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información.
- La Oficina TIC establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.
- Cualquier producto software que opere en la Administración Municipal deberá contar con el aval de la Oficina de Tecnologías de la Información y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

6.9 Políticas para Teletrabajo

La modalidad de trabajo a distancia, o teletrabajo, trae consigo nuevas amenazas asociadas a la seguridad de la información. Es por eso que se deben establecer los protocolos adecuados para mitigar los riesgos subyacentes y relacionados con el traslado de la información a nuevas ubicaciones físicas:

- Si la terminal de trabajo es propiedad de la Administración Municipal, se deben tener en cuenta las disposiciones del punto 6.3.7Dispositivos móviles.
- Con el fin de llevar un registro claro de los empleados y contratistas que estarán en teletrabajo, el jefe de la dependencia u oficina que autorice a uno o varios colaboradores suyos a usar esta modalidad de trabajo, deberá hacer llegar a la Oficina de Tecnologías de la Información y las Comunicaciones la relación de dicho personal. Esta relación debe tener, como mínimo, la siguiente información:
  - Nombre y cargo del colaborador
  - Fecha de inicio y de terminación de teletrabajo
  - Días de la semana y horario para teletrabajo
  - Aplicaciones de la entidad que usará mientras esté en teletrabajo
  - Si usará una terminal propia o provista por la entidad
  - En caso de terminal propia, indicar si ésta tiene licencias legales del sistema operativo, de la aplicación de ofimática, de la solución antivirus y de cualquier otra aplicación con la que se procese, almacene o comunique información de la entidad
- Por parte de la Oficina de Tecnologías de la Información y la Comunicaciones, se debe...
  - Llevar a cabo una revisión tanto de la terminal desde donde se conectará el usuario de teletrabajo para verificar las condiciones eléctricas, de licenciamiento y de seguridad del puesto de trabajo, entre otras.
  - Establecer e implementar los parámetros necesarios para garantizar la seguridad en la comunicación (VPNs, VLANs, etc.)
  - Llevar a cabo las tareas de soporte necesarias para garantizar la disponibilidad de los equipos y servicios propiedad de la entidad.
- El usuario, por su parte, debe cumplir con las siguientes obligaciones
  - Las sesiones abiertas de forma remota solo deben ser usadas por el colaborador a quién se autorizó el teletrabajo.

- No se debe hacer teletrabajo conectado a redes públicas como un café internet, zonas wifi, restaurantes, etc.
- Cumplir con las condiciones de fechas y horarios indicados en la relación que se traslada a la Oficina TIC
- Cumplir con las políticas establecidas más adelante como 6.15 Políticas Adicionales.
- Reportar a la Oficina TIC cualquier evento referente a la pérdida de confidencialidad, pérdida de integridad o pérdida de disponibilidad de los recursos asignados.

6.10 Disponibilidad del Servicio e Información

La Alcaldía Municipal de Guadalajara de Buga velará por implementar un plan de continuidad del negocio, proporcionando los recursos necesarios para mantener niveles óptimos de disponibilidad de servicios e información para los procesos que soporta el Sistema de Seguridad de la Información, incluyendo los servicios provistos por terceros.

El plan de continuidad debe tener en cuenta los siguientes parámetros:

- **Niveles de disponibilidad**. El plan de continuidad permitirá asegurar que se cumpla un mínimo de disponibilidad. Estos niveles mínimos se acordarán con usuarios, proveedores y/o terceros y calcularán con base en la criticidad del activo de información, teniendo en cuenta las necesidades de la entidad, los acuerdos de nivel de servicio y las evaluaciones de riesgos.
- **Planes de recuperación**. Se deben construir planes de recuperación teniendo en cuenta los niveles de disponibilidad establecidos.
- **Acuerdo de Nivel de Servicio**. Se deben establecer Acuerdo de Nivel de Servicio (ANS) tanto de los proveedores de servicios con la entidad como de la entidad con los clientes internos y externos. Estos ANS definirán tanto los estándares de servicio que el proveedor del mismo está obligado a cumplir como las responsabilidades del cliente.
- **Interrupciones**. Se deben tener procedimientos que permitan gestionar las interrupciones programadas de mantenimiento que afecten la disponibilidad de servicios e información. En los procedimientos para gestionar las interrupciones, se debe tener presente los Acuerdos de Nivel de Servicio (ANS).
- **Segregación de ambientes**. Para minimizar el riesgo de puesta en marcha de nuevos desarrollos e implementaciones se debe recurrir a la «segregación de ambientes» que permitan aislar cambios y desarrollos en período de prueba, antes de ser trasladados a producción.
- **Gestión de cambios**. Se deben implementar procedimientos de control o gestión de cambios en los sistemas de información, que permitan minimizar la afectación a la disponibilidad en el momento de su paso a producción. Esta gestión de cambios debe exigirse también a proveedores de sistemas de información externos.

6.11 Registro y Auditoría

La Administración Municipal de Guadalajara de Buga debe mantener evidencia de las actividades y acciones que afecten a los activos de información. Es responsabilidad de la Oficina de Control Interno Administrativo el realizar las auditorías periódicas correspondientes a los sistemas y actividades relacionadas con la gestión de activos de información e informar sobre los resultados de dichas auditorías.

Para este ítem, se debe tener en cuenta lo siguiente:

- El Comité de Seguridad de la Información determinará los eventos que deben dar lugar a registros de auditoría en los recursos tecnológicos y los sistemas de información de la entidad.
- La dependencia custodia del activo de información o el proveedor de servicio correspondiente, debe implementar los registros de auditoría para los eventos definidos por el Comité de Seguridad. Estos registros de auditoría sólo podrán ser accedidos por funcionarios autorizados para su monitoreo y evaluación.
- Los registros de eventos sobre las bases de datos deben incluir los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de la misma.
- Se deben programar, con cierta periodicidad, monitoreos a los registros de auditoría generados y analizar los resultados para detectar eventos de seguridad indeseados.
- Las auditorías al Sistema de Seguridad y Privacidad de la Información deben realizarse de acuerdo a la normatividad vigente y a los requerimientos legales aplicables a la naturaleza de la entidad. Estas auditorías deben garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la entidad, así como recomendar las deficiencias detectadas.
- La periodicidad de las auditorías debe ser tal que permitan la revisión de los niveles de riesgos a que está expuesta la entidad, lo que se logra alineando estas auditorías a los objetivos estratégicos y a la gestión de procesos.

6.12 Gestión de Incidentes de Seguridad de la Información

La entidad debe establecer procedimientos que permitan gestionar de forma eficiente los eventos, incidentes y vulnerabilidades de seguridad de la información. Estos procedimientos deben estar dirigidos a todos los funcionarios responsables de la información y a quienes tengan acceso autorizado a cualquier sistema de información y deben también estar aprobados por la alta dirección, quien certificará así su compromiso con el proceso.

- La Administración Municipal promoverá entre los empleados, contratistas y terceros el reporte y seguimiento de eventos, incidentes y vulnerabilidades relacionados con la seguridad y la privacidad de la información. Los eventos, incidentes o vulnerabilidades identificadas por el funcionario, deben ser reportadas a la Oficina TIC por cualquier medio habilitado por ésta. De igual manera, se debe promover el reporte al líder de área de la pérdida o divulgación no autorizada de información clasificada como de uso interno o confidencial.
- La Oficina TIC debe asignar responsables para el tratamiento de los incidentes, eventos o vulnerabilidades identificados por ellos mismos o reportados por otros funcionarios. Estos responsables del tratamiento deben realizar las averiguaciones pertinentes y llevar a cabo las acciones necesarias para eliminar el suceso y/o mitigar el impacto de este sobre los activos de información y para evitar su reincidencia. El Comité de Seguridad de la Información designará, en conjunto con el líder de la Oficina TIC, a un profesional calificado como responsable para la gestión de incidentes y vulnerabilidades de seguridad, en colaboración con personal auxiliar o contratista. También, este Comité designará al responsable para la gestión de incidentes relacionados con la pérdida o divulgación no autorizada de información.
- Los responsables del tratamiento deben llevar un registro de todas las actividades que rodean el evento de seguridad, desde el reporte o identificación del mismo, hasta la manera de resolución o mitigación. Igualmente, se debe mantener una «base de conocimiento» para los incidentes de seguridad más significativos con sus respectivas soluciones, a fin de reducir el tiempo de respuesta cuando se vuelvan a presentar.
- La Administración Municipal velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, privacidad de la información y con la referente a derechos de autor, propiedad intelectual, ley de transparencia y del derecho de acceso a la información pública

nacional, para lo cual tanto la Oficina Jurídica como la Oficina TIC deben mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la entidad y relacionados con estos temas.

6.13 Capacitación y Sensibilización en Seguridad de la información

La alta dirección de la Alcaldía Municipal de Guadalajara de Buga debe destinar los recursos necesarios para desarrollar programas de capacitación y sensibilización en temas de seguridad y privacidad de la información, con el objetivo de disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. Para planificar estos programas, debe tenerse en cuenta el documento «Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información» publicado por el Ministerio TIC en el siguiente enlace: https://www.mintic.gov.co/gestionti/615/artic 5482_G14_Plan_comunicacion_sensibilizacion.pdf. También deben respetarse los siguientes lineamientos:

- La Entidad debe diseñar programas de capacitación o entrenamiento para todos aquellos funcionarios que, para llevar a cabo sus funciones, necesiten afianzar o adquirir nuevas habilidades en temas de seguridad y privacidad de la información. Aunque estos funcionarios son generalmente personal de TI o responsables de la seguridad y/o tratamiento de datos personales, en casos especiales puede requerirse entrenar a otros usuarios en temas afines.
- La Administración Municipal debe diseñar programas de sensibilización para todos y cada uno de los funcionarios la Entidad, con el objetivo de enseñar o reforzar buenas prácticas en temas de seguridad y privacidad de la información.
- La asistencia a los cursos o eventos de capacitación y sensibilización debe ser de carácter obligatorio y la Administración Municipal debe prestar su apoyo logístico y de recursos para llevarlos a cabo.
- Se harán revisiones periódicas, mediante el uso de métricas, a los resultados de la sensibilización y las capacitaciones para elaborar planes de mejoramiento sobre estas.
- El profesional de la seguridad de la información será quien diseñe y comunique los programas de capacitación y sensibilización. De igual manera, será él quien realizará o delegará la elaboración de la documentación sobre planes de estudio y desarrollo de programas.
- El personal ya capacitado y/o sensibilizado debe asumir su compromiso con la preservación de la seguridad de la información en la Entidad. Este compromiso se hará por escrito y podría realizarse a través de cláusulas en los formatos de asistencia a los eventos de capacitación/sensibilización que indiquen que han recibido los conocimientos pertinentes.
- Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad.

6.14 Políticas Especiales para Terminales de Áreas Financieras

Las terminales fijas y móviles utilizadas para transacciones financieras, como son pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otras, requieren lineamiento especiales que eleven aún más su nivel de seguridad. A continuación se presentan los requerimiento mínimos adicionales a los ya expuestos anteriormente y que deben cumplir las entidades públicas de orden nacional y territorial en los equipos y terminales que se usan para transacciones financieras con recursos públicos, a través de los portales de Internet que las entidades bancarias disponen para tal fin:

- **Lineamiento adicionales de seguridad lógica**

- Requerir, para el uso del dispositivo, mayores especificaciones de seguridad en las credenciales de acceso (mayor longitud mínima en las contraseñas o uso de caracteres especiales en las mismas, por ejemplo), las cuales deberá obligarse a ser cambiadas con mayor regularidad.
- Limitar los privilegios de las cuentas de usuario utilizadas para realizar transacciones financieras a fin de reducir el riesgo de instalación de software malintencionado o controladores de dispositivos no autorizados.
- Restringir, en lo posible, la ejecución de archivos como aquellos con extensiones .exe, .vbs, .com .scr, etc., y que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo electrónico por parte del usuario.
- Establecer procedimientos, automáticos o no, para efectuar, semanalmente, el borrado de todo tipo de archivos temporales, cookies, historial de navegación, y descargas.
- Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de Software o Hardware en estos equipos de cómputo o terminales móviles, sólo sean realizadas por personal autorizado de la Oficina TIC. Estas actividades deben ser revisadas y aprobadas por el PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN de la Entidad.
- Restringir la instalación de Software que permita conexiones remotas (Temaviewer, Anydesk, LogMeIn, Hamachi, VCN, entre otros), evitando con esto que personas externas no autorizadas se puedan conectar fácilmente a estos dispositivos. Igualmente, se debe restringir el Software de acceso remoto que pueda tener preinstalado el sistema operativo.
- Se debe asegurar que el Sistema Operativo mantenga actualizado a cada momento y el Antivirus, además de estar debidamente licenciado, debe contener módulos anti-keylogger, anti-spyware y de cortafuegos personal.
- Se deben restringir los puertos que permitan conectar dispositivos de almacenamiento extraíbles (USB, CD/DVD, SD Card, etc.), sin perjuicio del uso de dispositivos para la seguridad de transacciones como tokens.
- Procurar tener instalado un sólo navegador web en el que esté comprobada la adecuada compatibilidad y operación de servicios en línea de las entidades financieras, realizando la configuración de seguridad adecuada del mismo y asegurando su constante actualización. Esto para efectos de minimizar la cantidad de vulnerabilidades propias de los navegadores web.
- Mantener activos sólo los puertos, protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades.
- En lo posible, el equipo o dispositivo debe destinarse sólo para realizar las transacciones financieras y debe tener una conexión a Internet independiente y no compartida.

- **Lineamientos adicionales de seguridad física**

  - El área física en donde se realizan las transacciones financieras debe ser restringida sólo a personal autorizado.
  - Se debe limitar el uso de terminales móviles corporativas para realizar transacciones financieras. En caso de que sean absolutamente necesarias y estas deban trasladarse fuera de la Entidad, deben tomarse todas las medidas necesarias para evitar el acceso a personas no autorizadas o, en caso de pérdida o hurto, deberán mantenerse separados los mecanismos de seguridad que habiliten la ejecución de transacciones, como tokens o llaves de seguridad.
  - En lo posible, contar con cámaras de video que cubran al menos el acceso principal al área y el funcionario que utilice el equipo o terminal móvil. Las imágenes deberán ser conservadas por al menos seis meses o, si la imagen es objeto de alguna reclamación, queja o cualquier proceso de tipo judicial, hasta el momento en que este sea resuelto.

- **Lineamientos adicionales de seguridad de la red**

  - Se debe restringir totalmente el acceso a correos electrónicos personales, redes sociales y, en general, a otros sitios no asociados con las funciones del operador.
  - Implementar mecanismos de autenticación que permitan confirmar que el equipo o terminal móvil es un dispositivo autorizado dentro de la red de la Entidad, evitando así suplantaciones.
  - En el caso de dispositivos móviles, se debe evitar la realización de transacciones desde conexiones públicas o de terceros no confiables. Las redes inalámbricas confiables deben contar con las mejores condiciones y estándares técnicos disponibles, con usuario y contraseñas robustas que se cambien periódicamente.

- **Lineamientos adicionales frente a la entidad financiera**
  - Al equipo o terminal móvil en el que se realicen las transacciones financieras se deberá asignar una dirección IP pública fija, distinta a la utilizada para otros servicios de la Entidad.
  - Las contraseñas de ingreso a los equipos y dispositivos móviles usados para realizar transacciones financieras deben ser única y personalizada. No se deben usar contraseñas genéricas, compartidas o para grupos.
  - Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.

- **Lineamientos adicionales de seguimiento y monitoreo de controles**
  - El máximo responsable del área financiera de la Entidad, deberá coordinar con las áreas de TI y/o de seguridad de la información y/o las Oficinas de Control Interno, el responsable de verificar el cumplimiento de las condiciones de seguridad del equipo y en general, las consagradas en este instructivo, al menos cada tres (3) meses.
  - Para la verificación del cumplimiento de las condiciones de seguridad y los lineamientos aquí establecidos, se deberá diligenciar un documento con la lista de chequeo que contenga los controles adicionales aquí establecidos. Este documento deberá ser suscrito tanto por el responsable del área financiera, como por el designado para la respectiva verificación.

6.15 Políticas Adicionales

Estas políticas adicionales se relacionan directamente con el debido comportamiento de los usuarios.

6.15.1 Política de Uso aceptable

Todos los funcionarios y contratistas que hagan uso de los recursos tecnológicos propiedad de la Alcaldía Municipal de Guadalajara de Buga, tienen la responsabilidad de cumplir cabalmente las siguientes políticas que propenden por un uso adecuado de los mismos, minimizando así traumatismos en la continuidad de las operaciones en la Entidad.

- **Políticas sobre el uso de los recursos tecnológicos**
  - Los activos tecnológicos serán de la completa responsabilidad del funcionario o contratista al cual han sido asignados y este los utilizará únicamente para el desempeño de las labores propias de su cargo o actividades. Por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Oficina TIC, salvo que medie alguna solicitud formal del jefe de área.

- Sólo se permite el uso de software debidamente licenciado por la Entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Oficina TIC.
- No se conectarán a la red interna de la Alcaldía Municipal de Guadalajara de Buga o de alguna de sus oficinas externas, ya sea por cable o de forma inalámbrica, equipos de cómputo o dispositivos que no sean de propiedad de la Entidad. En caso de que se deba hacer uso de uno de esos equipos, será de manera temporal durante el mismo día y la Oficina TIC deberá avalar primero que el mismo cumpla con la legalidad del software instalado, que tenga software antivirus debidamente licenciado y actualizado y que esté libre de software malicioso.
- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas en custodia al líder de área o a la Oficina TIC cuando finalice su vinculación con la Entidad. La Administración Municipal debe garantizar que este procedimiento se lleve a cabo.
- Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- No se deberá ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de integridad y disponibilidad de ésta.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro de energía, salvo los que estén autorizados expresamente.
- No está permitido conectar dispositivos de red que permitan la derivación de nuevas conexiones, como conmutadores (switches) o concentradores (hubs), ya que estos redundan en la degradación del rendimiento general de la red, salvo los autorizados expresamente por la Oficina TIC.
- Las únicas personas autorizadas para realizar revisiones, modificaciones, actualización y reparaciones a nivel de Hardware o Software en los elementos o recursos tecnológicos de la Administración Municipal, son las designadas para tal labor por la Oficina TIC.
- La Oficina TIC es la única dependencia autorizada para administrar el Software de la Entidad, el cual no deberá ser copiado, entregado a terceros ni utilizado para fines personales.
- La única dependencia autorizada para trasladar los elementos o recursos tecnológicos de un puesto a otro es la Oficina TIC, con el fin de llevar el control de inventarios de los mismos. El procedimiento para la asignación o reasignación de equipos deberá acordarse con el área de Almacén.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá reportarse de inmediato a la Oficina TIC de la Entidad por el funcionario o contratista a quien se asignó. La Oficina TIC, a su vez, deberá reportar el incidente tanto a la Dirección Administrativa como a la Secretaría de Desarrollo Institucional siguiendo los procedimientos establecidos para este tipo de siniestros.
- La pérdida de información deberá ser informada con detalle a la Oficina TIC y el caso deberá crearse en el sistema de Mesa de Ayuda como incidente de seguridad.
- Todo incidente de seguridad que comprometa la integridad, la confidencialidad y la disponibilidad de la información deberá ser reportado a la mayor brevedad a la Oficina TIC, y el caso deberá registrarse en el sistema de Mesa de Ayuda.
- Todo acceso a la red de la Entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la Oficina TIC.
- En caso de que exista una red inalámbrica para uso de funcionarios y contratistas de la entidad, ésta será administrada por la Oficina TIC, quien tomará las medidas para dotar de la seguridad necesaria que minimice los incidentes de seguridad por su uso.

  - El acceso a la red inalámbrica por parte de visitantes de la Entidad también estará controlado por la Oficina TIC. Esta red estará completamente aislada y segmentada de la red LAN de la Entidad, tendrá una identificación (SSID) distinta a la red para funcionarios y contratistas y tendrán contraseñas dinámicas que deberán ser cambiadas semanalmente y que sólo estarán disponibles en el horario laboral.
  - Los equipos de cómputo deberán ser apagados cada vez que el usuario esté ausente o durante la noche, con el fin de proteger la seguridad de los recursos. Igualmente, si el usuario debe ausentarse por un momento, deberá bloquear el acceso al recurso para garantizar la confidencialidad de la información.

- **Políticas sobre el uso de los sistemas de información**
  - Las credenciales de acceso a los sistemas de información y aplicaciones (usuarios y contraseñas) son de uso personal e intransferible. Los funcionarios y contratistas no deben revelar estos datos a terceros ni utilizar credenciales ajenas.
  - Los funcionarios y contratistas son responsables por el cambio periódico de sus contraseñas de acceso.
  - Todo funcionario o contratista es responsable de los registros, modificaciones y eliminación de información que se hagan con sus credenciales.
  - Ante la ausencia prolongada de un funcionario o un contratista, y si el líder de área así lo requiere, el acceso a su estación de trabajo será bloqueada mediante una solicitud hecha a la Oficina TIC, con el fin de evitar la exposición de información y el acceso de terceros que pueden generar daño, alteración o uso indebido, así como la suplantación de identidad.
  - Cuando un funcionario o contratista cesa sus funciones o culmina la ejecución de un contrato con la Entidad, todos los privilegios sobre cualquier recurso informático deben ser suspendidos inmediatamente.
  - Todos los servidores públicos o contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la ley 23 de 1982 y la Ley 44 de 1993 sobre derechos de autor, el Decreto 1474 de 2002 del Ministerio de Relaciones Exteriores, la Decisión 251 de 1993 de la Comunidad Andina de Naciones, así como cualquiera otra que adicione , modifique o reglamente la materia.

- **Políticas sobre el uso de Internet**
  - La Administración Municipal, a través de la Oficina TIC, debe monitorear el uso de Internet, además de limitar el acceso a determinadas páginas, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.
  - La Oficina TIC establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones.
  - Los servicios de Internet a los que un funcionario o contratista tenga acceso, dependerá del rol o funciones que desempeñe dentro de la Entidad y para las cuales esté formal y expresamente autorizado por su jefe o supervisor, y solo se utilizará para fines laborales.
  - Los funcionarios y contratistas deben abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
  - Está prohibido por parte de funcionarios y contratistas de la Administración Municipal visitar sitios web que ofrezcan servicios de streaming de audio y video ya que esto atenta contra la disponibilidad y rendimiento del servicio de banda ancha necesario para que otros usuarios puedan realizar sus labores. Se exceptúa esta prohibición para funcionarios y contratistas de la oficina de comunicación y prensa y de la Oficina TIC que lleven a cabo labores o actividades en estas plataformas necesarias para la Entidad.

- Los funcionarios y contratistas deben abstenerse acceder a sitios web, portales, o aplicaciones web que no hayan sido autorizadas por las políticas de la Entidad.
- Los funcionarios y contratistas deben abstenerse de enviar y descargar cualquier tipo de Software o archivo de fuentes externas de procedencia dudosa o desconocida.
- Los funcionarios y contratistas deben abstenerse de propagar intencionalmente virus o cualquiera tipo de código malicioso.

- **Políticas sobre el uso del Correo Electrónico**
  - Los únicos correos electrónicos autorizados para el manejo o transmisión de la información institucional en la Entidad son los correos electrónicos institucionales autorizados por la Oficina TIC y que han sido asignados por la misma dependencia o por entidades de orden Nacional como el Ministerio de Tecnologías de la Información y las Comunicaciones o el Ministerio de Educación, y que cuentan con dominios como @guadalajaradebuga-valle.gov.co, @buga.gov.co, @bugadigital.gov.co, @sembuga.gov.co, etc. Esto se da por que estos buzones cumplen con los requerimientos técnicos y de seguridad que minimizan la probabilidad de ataques e infecciones por virus u otro Software malicioso.
  - El correo electrónico institucional debe ser utilizado únicamente para enviar y recibir mensajes de tipo institucional. No puede ser utilizado con fines personales, económicos, comerciales o cualquier otro fin ajeno a los propósitos de la Entidad.
  - Se debe restringir al máximo el uso de correos electrónicos personales. Esto evita la potencial descarga de virus o Software malicioso y la fuga de información por estos medios.
  - Está expresamente prohibido distribuir, copiar o reenviar información de la Administración Municipal de Guadalajara de Buga a través de correos electrónicos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
  - En cumplimiento de la iniciativa institucional del uso eficiente del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la Ley lo permita.
  - Los mensajes de correo están respaldados por la Ley 527 de 1999, la cual establece la legalidad de los mensajes de datos y las implicaciones legales por el mal uso de estos.
  - La Oficina TIC implementará las herramientas tecnológicas adecuadas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.
  - Se prohíbe el envío masivo de mensajes de correo electrónico que signifique SPAM y que no sean de interés real para el destinatario. La Administración Municipal definirá desde cuál o cuáles correos electrónicos institucionales se podrán realizar estos envíos masivos y con qué contenidos específicos.
  - La solicitud de correos electrónicos nuevos, o cambios en los ya existentes, debe hacerse mediante oficio a la Oficina TIC de la Entidad, en donde se relacionarán también los funcionarios que, en nombre del titular o líder de área o proceso, podrán escribir o responder en nombre de estos. Esto con el fin de mitigar problemas de suplantación.
  - Todo mensaje recibido que contenga SPAM o cadenas, de remitente o contenido sospechoso, debe reportarse inmediatamente a la Oficina TIC y deben acatarse las indicaciones recibidas para su tratamiento. Lo anterior, debido a que pueden contener virus, en especial si llevan archivos adjuntos. Está también expresamente prohibido el reenvío de este tipo de mensajes.
  - Las cuentas de correo electrónico institucional no deben ser revelados en sitios web o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, etc. o cualquier otra ajena a los fines de la entidad.
  - Está expresamente prohibido el envío de mensajes de correo electrónico con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y que atenten contra la integridad moral de las personas e instituciones.

- El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida sea catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.
- Todo correo electrónico institucional debe incluir el Aviso de Privacidad, contenido en el Anexo 1 del documento vigente de «Políticas para el Tratamiento de Datos Personales», de la Alcaldía Municipal de Guadalajara de Buga.
- Cuando un funcionario o contratista cesa en sus funciones o culmina la ejecución de un contrato con la Entidad, no se le entregará copia de sus buzones de correo electrónico institucional a su cargo, salvo autorización expresa de la alta dirección o por orden judicial.
- La Administración Municipal se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus funcionarios y contratistas. Además, podrá hacer copias de seguridad de estos correos en cualquier momento y sin previo aviso y limitar el acceso temporal o definitivo a estos servicios de ser necesario.

- **Políticas de uso de plataformas y redes sociales institucionales**
  - La plataforma web oficial de la Administración Municipal de Guadalajara de Buga es www.guadalajaradebuga-valle.gov.co. La Administración Municipal deberá indicar qué dependencia y/o funcionario será el responsable de la publicación en dicho sitio y qué dependencias y/o funcionarios podrán interactuar con la ciudadanía a través de esta plataforma (foros, chats, respuestas a consultas, etc.).
  - La Administración Municipal determinará de manera formal cuáles son las cuentas institucionales en las diferentes redes sociales que están autorizadas para la interacción con la ciudadanía e indicará claramente qué dependencia y/o funcionario será responsable de estas.
  - Queda expresamente prohibido a empleados, contratistas, aprendices y practicantes la publicación de información institucional en los canales oficiales. Esta publicación, además, deberá estar autorizada por el responsable de la cuenta. La prohibición no incluye el compartir contenido proveniente de una fuente institucional y que se considere de interés público.

- **Políticas de uso eficiente del papel**

  Estas políticas propenden por el uso eficiente del papel, lo que ayuda a mantener la seguridad y privacidad de la información, ya que es más fácil para una organización gestionar la información almacenada en medios electrónicos que en medios físicos.

  - Los usuarios de la Administración Municipal deberán utilizar siempre la impresión y fotocopia a doble cara, con excepción de aquellos casos en que normas internas, como las del Sistema de Gestión de Calidad, Programa de Gestión Documental, o requerimientos externos, exijan el uso de una sola cara de la hoja.
  - Los usuarios de la Administración Municipal utilizará, en lo posible, las funciones que permiten reducir los documentos a diferentes tamaños, de tal forma que en una cara de la hoja quepan dos o más páginas. Para revisión de borradores resulta muy apropiado.
  - Los usuarios de la Administración Municipal intentarán elegir el tipo de letra más pequeño posible en la impresión de borradores (por ejemplo 10 puntos). En las versiones finales o en documentos oficiales deberán utilizarse las fuentes y tamaños determinados por el Sistema de Gestión de Calidad o las normas relacionadas con estilo e imagen institucional.
  - Para evitar desperdicios de papel, los usuarios de la Administración Municipal deben tomarse al tiempo suficiente para hacer la revisión y corrección en pantalla del documento y deben asegurarse que el documento esté bien configurado antes dar la orden de impresión, utilizando para ello las herramientas de revisión y vista previa. En el caso de los borradores o documentos internos pueden usarse márgenes más pequeños. En los informes y oficios definitivos se deben utilizar los márgenes definidos por los manuales de estilo y directrices del Sistema de Gestión de Calidad.

- Los usuarios de la Administración Municipal debe evitar las copias e impresiones innecesarias. Es importante determinar, antes de crear o generar múltiples ejemplares de un mismo documento, si son realmente indispensables. En la mayoría de los casos existen medios alternativos para compartir o guardar copias de los documentos de apoyo tales como el correo electrónico, la intranet, repositorios de documentos o carpetas compartidas.
- En los casos que no se requiera copia impresa de los documentos, se recomienda almacenarlos en el disco duro del computador, discos compactos, DVD u otro medio tecnológico que permita conservar temporalmente dicha información. Es importante que la Entidad cuente con políticas claras sobre la forma de nombrar, clasificar y almacenar documentos digitales, con el fin que puedan ser preservados y garanticen su recuperación y acceso para consulta. En este aspecto es importante que los servidores públicos adopten las directrices formuladas por el Comité de Archivo de la Entidad, utilizando las recomendaciones y normas que en materia de preservación digital emita el Archivo General de la Nación.
- Todos los usuarios de la Administración Municipal deben conocer el correcto funcionamiento de los equipos de impresión y fotocopiado, para evitar el desperdicio de papel que se deriva de su mala utilización.
- Los usuarios de la Administración Municipal deben utilizar las hojas de papel usadas por una sola cara para la impresión de borradores, toma de notas, impresión de formatos a diligenciar de forma manual, listas de asistencia, entre otros.

6.15.2 Política de Escritorio Limpio y Pantalla Limpia

Esta política busca evitar el acceso no autorizado o la pérdida, fuga o daño de información de la Entidad que se encuentra sobre los puestos de trabajo o en el escritorio del sistema operativo, tanto dentro como fuera del horario laboral. Son de obligatorio cumplimiento para funcionarios y contratistas de la Administración Municipal, pues es responsabilidad de estos minimizar la exposición de información sensible.

- Al ausentarse del puesto de trabajo o al finalizar la jornada laboral, los escritorios deben permanecer limpios y libres de documentos físicos o de dispositivos de almacenamiento externo (memorias USB, discos duros externos, CDs, DVDs, etc.), donde repose información de la Entidad. Estos documentos y dispositivos deben almacenarse bajo llave y en lugares adecuados que eviten el deterioro por humedad u otras condiciones ambientales.
- Equipos móviles como tabletas, celulares o PCs portátiles deben permanecer bajo llave cuando no se estén utilizando. Estos últimos deben mantener asegurados con cables de seguridad cuando estén en uso para evitar robos.
- Al realizar impresión o digitalización de documentos, se debe asegurar que estos no permanezcan en los dispositivos tiempos prolongados que faciliten la pérdida de confidencialidad o disponibilidad. Es decir, los documentos deben retirarse de forma inmediata de los equipos cuando termine la impresión o digitalización. Estos equipos deben deben permanecer libres de documentos.
- El escritorio del sistema operativo utilizado en el equipo de cómputo (Microsoft Windows, Linux, MAC) debe estar libre de archivos y documentos. Sólo debe contener los accesos directos a las aplicaciones.
- Todos los equipos de cómputo deben estar protegidos con contraseñas que impidan el uso no autorizado de estos. Al levantarse del puesto de trabajo, el usuario debe bloquear su sesión a través de los mecanismos dispuestos en cada sistema operativo (*Windows+L*, en el caso de Microsoft Windows). También se debe implementar, por parte de la Oficina TIC, el bloqueo automático de la sesión en cada equipo de cómputo de la Entidad cuando pasen cinco minutos de inactividad.

- La Oficina TIC mantiene la potestad de intervenir cualquier equipo de cómputo, aun si estos están protegidos con contraseña, cuando se necesite acceder al mismo y el responsable no quiera permitirlo o se haya ausentado de manera temporal o definitiva de su cargo y no haya dado sus credenciales.
- Las sesiones remotas a servidores o equipos de trabajo de la entidad deben limitarse al mínimo necesario. Cuando se lleven a cabo, el usuario debe asegurar el bloqueo o terminación de dicha sesión al ausentarse del puesto de trabajo. Las sesiones deben bloquearse automáticamente después de cinco minutos de inactividad y, al reintentar la conexión, el sistema deberá solicitar de nuevo las credenciales de acceso.
- No se deben imprimir documentos de forma innecesaria. Las notas, adhesivas o no, con información importante (como nombres de usuario o contraseñas, direcciones IP, números de cuentas, datos personales, datos de propiedad intelectual, etc.) no se deben dejar a la vista, en los monitores o debajo de los teclados.
- Todos los equipos de cómputo y dispositivos de impresión y digitalización, deben apagarse cuando no estén en uso.

La aplicación de estas políticas debe revisarse, al menos, una vez al año con el fin de asegurar su eficiencia y efectividad y podrán ser actualizadas cuando se requiera.