#Soyedeso

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

2024

edeso
Empresa de Desarrollo Sostenible

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

TECNOLOGÍAS DE LA INFORMACIÓN (TIC´s)

EMPRESA DE DESARROLLO SOSTENIBLE EDESO

ENERO DE 2025

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

¿PARA QUÉ Y COMO SE HACE?

Para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Sé encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital. Y Se desarrolla mediante el Documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación. Lo debe desarrollar el líder o encargado de Seguridad de la Información con el apoyo de toda la estructura organizacional.

INTRODUCCIÓN

La empresa de Desarrollo Sostenible del Oriente, en adelante EDESO, está comprometida a proteger los activos de información de la entidad (empleados, colaboradores, contratistas, clientes, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, para la puesta en marcha y a la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de cultura y consciencia de seguridad de los funcionarios, contratistas, proveedores, clientes y personas que hagan uso de la EDESO.

En Colombia se viene implementando la política de Gobierno Digital, definida en dos componentes: TIC para el Estado y TIC para la sociedad, que son habilitados por tres transversales: Seguridad de la información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares requerimientos mínimos del sujeto obligado.

El CONPES 3854 define entorno digital como ambiente tanto físico, como virtual, sobre el cual se soporta el desarrollo de una economía digital sólida y segura es primordial para el país.

OBJETIVO GENERAL

Establecer las actividades que estén contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de Servicio, el Mapa de Procesos de la Empresa de Desarrollo Sostenible del Oriente (Edeso) y el Plan Estratégico de la Empresa.

OBJETIVOS ESPECIFICOS

- Mantener los lineamientos establecidos para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la Empresa de Desarrollo Sostenible, de acuerdo con los requerimientos establecidos en el modelo de seguridad y privacidad de la información bajo los estándares que exige la estrategia de Gobierno Digital.

- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación.

- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.

- Generar conciencia de los cambios organizacionales requeridos para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la Empresa de Desarrollo Sostenible.

- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

ALCANCE

Este Plan de Seguridad y Privacidad de la Información, aplica a todos los funcionarios de la Empresa de Desarrollo Sostenible del Oriente – EDESO, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la

entidad y terceras partes, que usen activos de información que sean propiedad de la Empresa.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Modelo de Seguridad y Privacidad de la Información MSPI, desde la Estrategia de Gobierno Digital contempla los siguientes ciclos de operación que contiene cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Estas fases del proceso

cumplen con el principio PHVA, ejecutando antes un diagnóstico general según la norma ISO 27001:2013, en el capítulo 4 -Contexto de la Organización.

DEFINICIONES

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos**: se refiere a 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 organismo. (CONPES 3854 de 20116).
- **Archivo**: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el

transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría**: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos**: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- **Datos Personales Mixtos**: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **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 de 2014. (Ley 1712 de 2014, art 6)

- **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 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC27000).

- **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada**: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- **Seguridad digital**: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder)**: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

BASE LEGAL

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, la confidencialidad y la trazabilidad de la información, se debe prever cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la información, entre otras, a lo establecido en las siguientes disposiciones legales: Marco normativo de buenas prácticas para el tratamiento de la información:

- Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Ley 1952 de 2019 Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.
- Decreto Nacional 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto Nacional 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto MinTIC 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

ROLES Y RESPOSABILIDADES

Es responsabilidad del área de TIC´s de la Empresa de Desarrollo Sostenible del Oriente – EDESO, la implementación, aplicación, seguimiento y autorizaciones del Modelo de Seguridad y Privacidad de la Información en las diferentes áreas y procesos de la Empresa, además garantiza el apoyo y el uso de la Política de Seguridad de la información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos misionales de la empresa.

COMUNICACIÓN

Mediante socialización a todos los funcionarios de La Empresa de Desarrollo Sostenible del Oriente - EDESO se dará a conocer el contenido del documento de las estrategias de seguridad y privacidad de la información, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la realimentación necesaria para dar cumplimiento efectivo al modelo.

Todos los funcionarios, contratistas y/o terceros de la Empresa deben conocer la existencia de las estrategias, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página institucional www.edeso.gov.co.

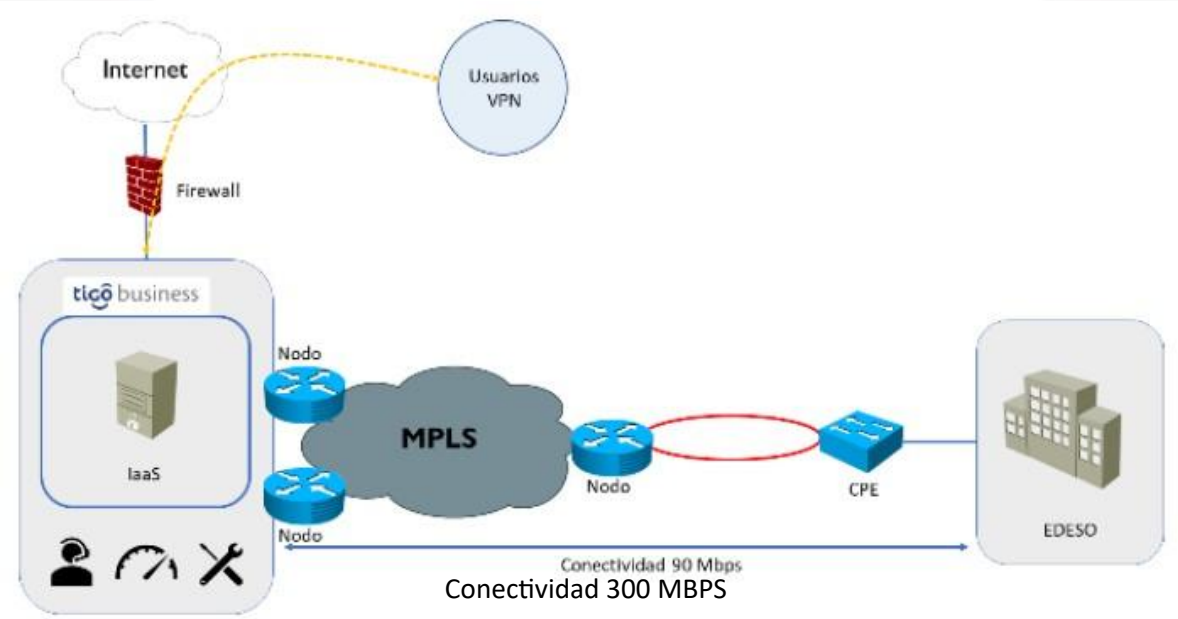
DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD

La información es uno de los activos más importantes de una organización por o que su integridad, confidencialidad y disponibilidad debe, de cierta manera, estar bajo un nivel adecuado de seguridad aceptable, cumpliendo con códigos de buenas practicas de seguridad de la información.

La Empresa de Desarrollo Sostenible del Oriente – EDESO, en todas sus áreas funcionales y procesos cuenta con información, reservada, relevante, restringida, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

TOPOLOGÍA DE SEGURIDAD Y CONTROL DE ACCESO A LA INFORMACIÓN

La Edeso ante su constante crecimiento y afán de proteger tanto los activos como la información con la cuenta actualmente, tiene un aliado tecnológico, que brinda seguridad y disponibilidad en 99.7%. Esta es su topología



Conectividad 300 MBPS

Se cuenta con un Firewall que se encarga de realizar todo el control de tráfico de información, desde y hacia las instalaciones de la Edeso.

GESTIÓN DE ACTIVOS

- IDENTIFICACIÓN, CLASIFICACIÓN Y CONTROL DE ACTIVOS DE INFORMACIÓN.

La Empresa de Desarrollo Sostenible – EDESO a través de los lideres y/o responsables de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El comité de archivo, con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la Empresa.

Siempre que se dé de baja un medio de almacenamiento como discos duros, memorias USB, entre otros, se debe destruir totalmente haciéndolos irrecuperables, así mismo debe quedar constancia de ello.

El procedimiento que se utilice para la eliminación del medio, deberá ser aquel que minimice el riesgo de fuga de información.

CONTROL DE ACCESO

- ACCESO A REDES Y RECURSOS DE RED

El líder de TIC´s de la Empresa de Desarrollo Sostenible del Oriente – EDESO, como responsable de las redes de datos y los recursos de red de la empresa, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

- ACCESO LÓGICO

La Empresa de Desarrollo Sostenible del Oriente – EDESO, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la empresa.

Los funcionarios, contratistas y el personal provisto por terceras partes deberán tener acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Los usuarios son responsables de la seguridad de sus contraseñas, tanto de su equipo como de los aplicativos a los cuales tiene acceso. Por ende, el usuario es responsable de todas las actividades realizadas con su nombre de usuario.

Los usuarios deberán cambiar su contraseña periódicamente y estas no deberán contener información personal como nombres o números de teléfono, con el fin de que no se pueda inferir la contraseña con dicha información.

Se debe evitar el almacenamiento de las contraseñas en papel o en registros digitales, a menos que estos tengan algún tipo de seguridad perimetral o de acceso.

Cuando un usuario olvide, bloquee o extravíe su contraseña deberá solicitar al Líder responsable en sistemas que le realice la acción que le permita ingresar una nueva contraseña, y al momento de recibirla deberá cambiarla por una nueva.

- CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN

La Empresa de Desarrollo Sostenible del Oriente – EDESO, como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El acceso a los sistemas de información críticos como el Software financiero, deberá ser accedido únicamente desde equipos seguros, en las instalaciones de la Empresa o equipos personales a través de VPN Seguras brindadas por el proveedor de servicios y Usando sus equipos personales, evitando el acceso desde equipos públicos o salas de internet.

Deberá evitarse el uso de la característica de los exploradores de “recordar usuario y contraseña”, para evitar que personas no autorizadas accedan a los sistemas de información valiéndose de esto.

Los accesos a sistemas de información WEB o aplicaciones WEB, deberán accederse digitando directamente la dirección en la barra de direcciones del explorador o siguiendo los enlaces seguros que a cada usuario le lleguen. En todo caso deberá evitar el uso de buscadores, marcadores o accesos directos.

Los usuarios deben finalizar las sesiones activas cuando finalice sus labores o dejar el equipo con en algún tipo de bloqueo cada vez que dejen el equipo desatendido.

- SEGURIDAD FÍSICA

La Empresa de Desarrollo Sostenible del Oriente – EDESO, vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Todos los servidores y los sistemas de procesamiento de información deberán contar con perímetros de seguridad física adecuados que impidan el acceso no autorizado al mismo.

Los dispositivos de red tales como routers, switchs, Access Point, etc., se consideran como área segura y deberá contener algún tipo de seguridad perimetral. En caso de no existir, los empleados contratistas o terceros deberán abstenerse de moverlo, reubicarlo o de conectarse directamente a él sin la autorización previa del líder responsable.

- SEGURIDAD PARA LOS EQUIPOS

La Empresa de Desarrollo Sostenible del Oriente - EDESO para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Cada equipo de cómputo incluyendo periféricos como scanner, impresoras y fotocopiadoras, deberán tener un responsable designado, al cual se le hará entrega formal del equipo por medio de un acta firmada por cada una de las partes, este documento deberá contener las características y el estado inicial del activo.

La ubicación de los equipos de escritorio y periféricos como impresoras, fotocopiadoras y scanner deberá ser la que menor riesgo tenga con respecto a posibles amenazas ambientales o accesos no autorizados, así mismo, el empleado o contratista deberá respetar dicha ubicación.

- USO ADECUADO DEL INTERNET

La Empresa de Desarrollo Sostenible del Oriente - EDESO consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores,

proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad, relacionadas netamente con las labores misionales de la empresa.

El acceso a Internet provisto para el personal de la Personería a través de la red es de uso exclusivo para el desarrollo de las actividades relacionadas con las necesidades del puesto y función que desempeña.

Los usuarios del servicio de la red de EDESO, al aceptar el servicio están aceptando que:

- Pueden ser sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descargar software sin la autorización del profesional responsable de la unidad sistemas.

- USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

La Empresa ha venido realizando inversiones importantes en la adquisición de una plataforma de correo electrónico robusta y con la suficiente capacidad y compatibilidad para cumplir los objetivos misionales de la empresa. Este se ha convertido en la principal herramienta de comunicación de la empresa, por lo que el uso responsable es prioridad de Todos.

- El correo electrónico institucional es personal e intransferible, cada usuario mantiene su propia cuenta y está prohibido el utilizar cuentas asignadas a otras personas para enviar o recibir mensajes de correo.
- El usuario debe utilizar el correo electrónico exclusivamente para desempeñar las funciones que le fueron asignadas por su cargo o empleo; cualquier otro uso del correo electrónico está prohibido.
- Los usuarios deben tratar los mensajes de correo electrónico institucional y archivos adjuntos como información de propiedad de la Empresa de Desarrollo Sostenible del Oriente - EDESO. Los mensajes de correo electrónico institucional deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- EDESO, se reserva el derecho a acceder y revelar todos los mensajes transmitidos por este medio para cualquier propósito, y revisar las comunicaciones vía correo electrónico institucional del personal que ha comprometido la seguridad, violado políticas de Seguridad Informática o realizado acciones no autorizadas.

CONTINUIDAD, CONTINGENCIA Y RECUPERACIÓN DE LA INFORMACIÓN

- COPIAS DE SEGURIDAD BACKUP

Se establecen los lineamientos para garantizar la información que se genera en cada una de las unidades de la Empresa de Desarrollo Sostenible del Oriente – EDESO

- Todos los funcionarios de la entidad que tienen a cargo equipos de cómputo y que manejen información importante y crítica son responsables de la seguridad de la misma.
- La información de los archivos contenidos en las copias de seguridad debe ser única y exclusivamente de uso institucional y no personal.
- En caso de que algún funcionario necesite copias de sus archivos almacenados en el servidor de Backup o en los medios de almacenamiento DVD, esta petición debe ser requerida al Profesional encargado de la Unidad de sistemas.
- Cada usuario es responsable de la información producida y derivada de su trabajo y de sus funciones. El usuario deberá realizar una copia de seguridad periódicamente de la información que consideren relevante y cuando el equipo sea enviado a mantenimiento, previendo así la pérdida involuntaria de información en el proceso de mantenimiento.
- En caso de solicitar la ejecución de una copia de respaldo, el profesional responsable de la unidad de sistemas solo estará obligado a rescatar la información pertinente a su labor más no a la información personal del usuario.

USO DE SOFTWARE

Cualquier instalación de software deberá ser realizado o, autorizado y aprobado por el profesional responsable de la unidad de sistemas.

Si se requiere el uso de software propietario, se deberá justificar el uso del mismo y solicitar la autorización al profesional responsable de sistemas indicando en que equipo o equipos deberá instalarse el programa.

El nivel de acceso que deberán tener los usuarios a sus equipos asignados, serán los mínimos que le permitan ejecutar de manera correcta y suficiente sus actividades diarias. En caso de que un usuario necesite privilegios de administrador en su sesión, ésta deberá ser aprobada y avalada por el profesional responsable de sistemas.

EVALUACIÓN DEL DESEMPEÑO DEL MSPI

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

- SEGUIMIENTO Y MEDICIÓN

Para las actividades de seguimiento y medición, la Empresa de Desarrollo Sostenible del Oriente - EDESO definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la administración municipal.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplimiento de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- Realizar ejercicios de auditoría interna del MSPI.

- Realizar actividades de revisión del MSPI por parte de la Subgerencia Administrativa y Financiera y la secretaría general.

MANTENIMIENTO Y MEJORA DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La empresa de Desarrollo Sostenible del Oriente – EDESO con la visión de mantenimiento y mejora de los aspectos de seguridad de la información, tendrá en cuenta los resultados de las evaluaciones iniciales del modelo, basado en los resultados de las actividades de seguimiento y medición (Indicadores)

La empresa de Desarrollo Sostenible del Oriente – EDESO

- Implementara las mejoras identificadas en el Modelo de Seguridad y Privacidad de la Información (MSPI)
- Identificará e implementará las mejoras identificadas en el Modelo de Seguridad y Privacidad de la Información (MSPI)
- Identificará e implementará acciones correctivas y preventivas que mitiguen situaciones de alto impacto.
- Implementará acciones de mejora basadas en las lecciones aprendidas de las experiencias de seguridad internas o de otras Empresas o Entidades.
- Asegurará que las mejoras cumplan con los objetivos y propósitos definidos por la Empresa de Desarrollo Sostenible del Oriente – EDESO

CRONOGRAMA MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

La empresa de Desarrollo Sostenible del Oriente – EDESO definirá y mantendrá un cronograma de actividades en cumplimiento a los propósitos internos de seguridad y privacidad de la información basada en el ciclo de operación del MSPI.

APROBACIÓN

El presente modelo de seguridad y privacidad de la información fue presentado y aprobado por el Comité Institucional de Gestión y Desempeño llevado a cabo el 28 de enero de 2025 según consta en acta de la misma fecha.

Elaboró: Juan Carlos Arroyave **Fecha:** 23/01/2024	**Revisó:** Subgerencia Administrativa y Financiera **Fecha:** 29/01/2024	**Aprobó:** Comité Institucional de Gestión y Desempeño **Fecha:** 29/01/2024