Nombre del documento	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
Estado del documento:	Versión liberada	
Responsables:	Nombre	Empresa
	Subdirección de Desarrollo y Tecnología	Unidad del Servicio Público de Empleo

Control de Versiones del Documento

Versión	Creación	Liberación	Descripción Cambio
1.0	Diciembre 2018	Enero 2019	Versión inicial
2.0	Enero 2020	Enero 2020	Actualización
3.0	Enero 2021	Enero 2021	Actualización

UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Unidad del Servicio Público de Empleo
Cra 69 No. 25B – 44 piso 7 Bogotá D.C.
PBX: (57 1) 7560009
www.serviciodeempleo.gov.co

Unidad del Servicio de Empleo

Tabla de Contenido

Unidad del Servicio Público de Empleo
Cra 69 No. 25B – 44 piso 7 Bogotá D.C.
PBX: (57 1) 7560009
www.serviciodeempleo.gov.co

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La definición de esta política es el primer paso para la implementación del Plan 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 en La Unidad Administrativa Especial del Servicio Público de Empleo en adelante la Unidad del SPE, con respecto a la protección de los activos de información de los funcionarios, contratistas, terceros. La información es un recurso que, como el resto de los activos tiene valor para la Entidad que por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Unidad del SPE.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional y para asegurar su cumplimiento, la dirección estratégica de la Entidad establecerá la compatibilidad de la Política de Seguridad de la Información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la Unidad del SPE
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Garantizar la continuidad del servicio frente a incidentes.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros y clientes de la Unidad del SPE.

1.1 Política General

La Unidad del SPE, reconoce la información como un activo estratégico para el cumplimiento de su misión y establece mecanismos con el propósito de preservar la confidencialidad, integridad y disponibilidad de esta, para asegurar la continuidad del servicio mediante criterios y procedimientos establecidos para funcionarios, contratistas y cualquier persona que tenga relación con la Entidad.

1.2 Objetivo General

La Unidad del SPE, busca establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, la protección, preservación, aseguramiento de la confidencialidad, integridad, disponibilidad, accesibilidad, legalidad y no repudio de los activos de información digital y física, enmarcado en el estricto cumplimiento de la normatividad, en concordancia con la misión y visión de la entidad y fortalecimiento de la cultura de la Seguridad de la Información, en funcionarios y contratistas.

1.3 Objetivos Específicos

- Establecer los fundamentos para el desarrollo del Modelo de Seguridad y Privacidad de la Información, con la norma ISO27001:2013.
- Definir la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.
- Establecer en los canales de comunicación que permitan a dirección mantenerse informada de los riesgos y uso inadecuado de los activos de información, y las acciones tomadas para su mitigación y corrección.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- Verificar los procedimientos manuales o automatizados que involucran intercambio de información.
- Divulgar en los funcionarios y contratistas La Política de Seguridad de la Información.
- Fomentar en los funcionarios y contratistas de la Unidad del SPE, las buenas prácticas y comportamientos seguros en el manejo de información.

2. ALCANCE/APLICABILIDAD

La presente Política de Seguridad de la Información, hace parte fundamental del Sistema Integrado de Gestión, donde se proporcionan las directrices a seguir para una información confiable, flexible y define el marco básico que guiará la implementación de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con la Seguridad de la Información, dentro de los procesos misionales, estratégicos y de apoyo definidos por la Unidad del SPE.

La presente aplica a la información sensible, procesada o utilizada en todos los niveles organizacionales de la Unidad del SPE, gestionada por los funcionarios, Contratistas, Proveedores, Entes de Control, Entidades Relacionadas y todos los que accedan de manera interna o externamente a cualquier activo de información, sin importar el medio, formato o lugar en el cual se encuentren.

2.1 Importancia De La Política De Seguridad De La Información.

Para la Unidad del SPE, es importante contar con la política de seguridad, ella guiará el comportamiento de funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada, así mismo la política permitirá que se trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales.

3. ORGANIZACIÓN Y RESPONSABILIDADES

La Secretaría General será el responsable de impulsar la implementación de la presente Política. Delegará o tendrá a cargo el mantenimiento y la presentación para la aprobación ante la máxima autoridad del organismo, el seguimiento de acuerdo con las responsabilidades propias de cada área de las actividades relativas a la seguridad de la información y la proposición de asignación de funciones.

La Subdirección de Desarrollo y Tecnología quien será responsable de la Seguridad Informática asistirá al personal de la Unidad del SPE en materia de seguridad de la información. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información y/o verificará la aplicación de las medidas de seguridad necesarias para la protección de esta.

La Secretaría General cumplirá la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las diferentes áreas.

La coordinación de contratación cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que estén relacionadas.

El supervisor del contrato notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información de la Unidad del SPE.

3.2 Responsabilidades frente a la seguridad de la información.

3.2.1 Responsabilidades Subdirección de Desarrollo y Tecnología.

- Establecer y mantener las políticas y procedimientos de servicios de tecnología, incluidos en esta política de seguridad de información, el uso de los servicios tecnológicos en toda la Unidad del SPE, de acuerdo con las mejores prácticas y lineamientos específicos de seguridad de la información para los procesos definidos en el Sistema Integrado de Gestión (SIG.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Unidad del SPE.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Unidad del SPE, a las diferentes Subdirecciones, así como a los entes de control e investigación que tienen injerencia sobre la entidad.
- La subdirección de Desarrollo y Tecnología prestará seguridad lógica y procedimentales para la protección de la información digital de la Unidad del SPE.
- Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la Unidad del SPE.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Unidad del SPE.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior la Unidad del SPE.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo.
- Implementar los mecanismos de controles necesarios para verificar el cumplimiento de la presente política.

- Garantizar la disponibilidad de los servicios, programar e informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de estos; así como gestionar su acceso de acuerdo con las solicitudes recibidas de las diferentes subdirecciones y coordinaciones siguiendo el procedimiento determinado.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, de acuerdo con las mejores prácticas y directrices de la Unidad del SPE.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos y las mejoras en los sistemas de información.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la Unidad del SPE.

3.2.3. Responsabilidades De Los Propietarios De La Información.

Son propietarios de la información cada una de las subdirecciones, así como las coordinaciones donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la entidad el acceso a la información de acuerdo con los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y las áreas que se encarguen de su protección y almacenamiento de acuerdo con las determinaciones y políticas de la Unidad del SPE, como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas.

4. CLASIFICACIÓN DE LA INFORMACIÓN

4.1 Información Pública

Toda información que la Unidad del SPE genere, adquiera, o controle, estará disponible para cada uno de nuestros usuarios y prestadores.

4.2 Información De Uso Interno

Toda información que se intercambia al interior de la Unidad del SPE, las características que se aplican son de disponibilidad, requiriendo el permiso y controles de accesos para los usuarios.

4.3 Información De Acceso Restringido

Toda información que se considere sensible determinada en Habeas Data debe controlarse su acceso a todos los usuarios.

5. POLÍTICAS ESPECÍFICAS

5.1 Política de seguridad:

- la Unidad del SPE, cuenta con firewall o dispositivo de seguridad para la conexión a internet.
- El usuario no debe interferir en los procesos computacionales de la Unidad del SPE, mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo, está prohibido el uso de aplicaciones o páginas de internet con el fin de tratar de burlar la seguridad o desempeño de la red interna institucional para acceder a sitios no autorizados y previamente bloqueados.

5.2 Política de la información:

La información sensible de la Unidad del SPE debe ser protegida sin importar su presentación, medio o formato en el que sea creada o utilizada para el soporte a las actividades de negocio. La seguridad de la información son el conjunto de medidas de protección que toma la Unidad del SPE contra la divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en el que se pueda ver comprometida la entidad.

Los dueños de la información son los responsables de asegurar y preservar la confidencialidad, integridad, disponibilidad y privacidad de esta. Cualquier persona que intente inhabilitar, sobrepasar cualquier control de seguridad será sujeto de una acción disciplinaria inmediata.

5.3 Seguridad De Los Recursos

La Unidad del SPE, a través de la Secretaria General propondrá que los servidores públicos, contratistas, usuarios y proveedores, entiendan su responsabilidad frente a la seguridad de la información, reduciendo el riesgo de robo, fraude, mal uso de la información, de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

5.4 Gestión De Activos De Información

- **Inventario de activos de información**: la Unidad del SPE debe hacer un inventario de los activos de la información sensible de la entidad.

  Además, con el objetivo de la implantación de controles de seguridad, las áreas organizacionales que son dueños de la información generada por los diferentes procesos de la entidad se encargarán de mantener y actualizar un inventario de activos de información relacionados con los servicios de cada dependencia, así como los servicios, software, hardware y recursos humanos, relacionados con ese proceso.

- **Archivos de gestión:** la Unidad del SPE, con el acompañamiento de la Subdirección de Desarrollo y Tecnología establecerán controles para garantizar que los archivos de gestión de la Entidad, cuente con los mecanismos de seguridad y así garantizar la protección y conservación de la información.

- **Responsabilidades de los funcionarios, contratista y colaboradores frente al uso de los Recursos Tecnológicos:** Todos los funcionarios, contratistas y colaboradores que hagan uso de los activos de información de la Unidad del SPE, tienen la responsabilidad de seguir la política establecida para el uso aceptable de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la continuidad de la misión institucional.

5.5 Uso del correo electrónico

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, contratistas y colaboradores de la Unidad del SPE, con los siguientes lineamientos:

- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la entidad.
- En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envió de documentos físicos.
- Los mensajes de correo electrónico están respaldados por la ley 527 de 1999 (por medio del cual se definen y reglamentan el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones), establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
- Todo mensaje de Spam o cadena debe ser reportado al correo helpdesk@serviciodeempleo.gov.co, como incidente de seguridad de la información, según procedimiento establecido.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado a helpdesk@serviciodeempleo.gov.co, como incidente de seguridad de la información según procedimiento establecido y proceder de acuerdo a las indicaciones de la Subdirección de Desarrollo y Tecnología; lo anterior porque puede ser contenido de virus, si este incluye archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .inf, .pif, tenga referencias no relacionadas con la Unidad del SPE.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional de la Unidad del SPE es el asignado por la Subdirección de Desarrollo y Tecnología y que cuenta con el dominio @serviciodeempleo.gov.co, el cual es el autorizado y cumple con los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

5.6 Mesa De Ayuda Tecnológica

Los servicios de mesa de ayuda son brindados para servicios estrictamente laborales, por consiguiente, cualquier servicio requerido deberá realizarlo a través del gestor de incidentes. Donde cada funcionario o contratista puede crear incidencias o requerimientos, categorizarlos, seleccionar el nivel de atención, describir la situación, entre otros aspectos necesarios para conocer la necesidad expuesta.

Toda solicitud de servicio de mesa de ayuda tecnológica será atendida conforme la priorización del servicio.

5.7 Uso Del Internet

La Unidad del SPE, a través de la Subdirección de Desarrollo y Tecnología, establecerá políticas de navegación basadas en categorías y niveles de usuario, jerarquía y funciones, previa validación del eje de seguridad de la información.

De acuerdo con el buen uso de los recursos de navegación de la Unidad del SPE, se deben tener en cuenta los siguientes lineamientos:

- El uso del servicio de internet está limitado exclusivamente para propósitos laborales.
- Los servicios a los que un determinado usuario pueda acceder desde internet dependerán de un rol o funciones que desempeña el usuario en la Unidad del SPE y para los cuales esté expresamente autorizados.
- Está expresamente prohibido él envió y/o descarga, visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web, aplicaciones web que no hayan sido autorizadas por la Unidad del SPE.
- Está expresamente prohibido la propagación de virus o cualquier tipo de código malicioso.
- La Unidad del SPE se reserva el derecho de monitorear los accesos, el uso del servicio de internet de todos sus funcionarios o contratistas, además de limitar el acceso a determinadas páginas de internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Unidad del SPE.

5.8 Uso de los Recursos Informáticos y/o Tecnológicos

Los recursos tecnológicos de la Unidad del SPE son herramientas de apoyo a las labores y responsabilidades de los funcionarios y contratistas. Por ello, está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el funcionario y contratista al cual han sido asignados, y únicamente para el correcto desempeño de las funciones del cargo o las obligaciones, por tanto, no pueden ser utilizados con fines personales o por terceros, no autorizados ante la Subdirección de Desarrollo y Tecnología, mediante solicitud formal a través de la mesa de ayuda.
- Es responsabilidad de los funcionarios y contratistas mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas a la Unidad del SPE, en custodia al finalizar vinculación laboral.
- Los funcionarios y contratistas no deben mantener almacenados en los discos duros de los equipos de cómputo de la Unidad del SPE o discos virtuales de red y/o servidores, archivos de video, música y fotos que no sean de carácter institucional.
- No está permitido realizar conexiones o derivaciones eléctricas por personal no autorizado, que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
- Los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Subdirección de Desarrollo y Tecnología.
- Los equipos deberán quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina, durante la noche, esto es con el fin de proteger la seguridad y distribuir bien el uso de los recursos, siempre y cuando no vaya a realizar alguna actividad vía remota.
- Se debe realizar análisis, monitoreo sobre los dispositivos de almacenamiento externos, con el fin de prevenir, detectar, fuga de información o infección de esta.
- La única dependencia autorizada para realizar respaldos de información de los servidores o de trasladar de un lugar a otro es la Subdirección de desarrollo y Tecnología, con el fin de llevar el control individual de inventario de información.

- La reasignación de equipos tecnológicos deberá ajustarse a los procedimientos y competencias de la Subdirección de Desarrollo y Tecnología.
- La pérdida o daño de elementos o recursos tecnológicos, o de algunos de sus componentes, debe ser informada de inmediato a la Subdirección de Desarrollo y Tecnología, por el funcionario o contratista a quien se le hubiere asignado.
- La pérdida de información debe ser documentada y reportada a la Subdirección de Desarrollo y Tecnología a través de la mesa de ayuda, como incidente de seguridad de la información.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado con el procedimiento establecido por la mesa de ayuda a la mayor brevedad posible.
- La Subdirección de Desarrollo y Tecnología a través de la mesa de ayuda son las únicas áreas autorizadas para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Todo acceso a la red de la Unidad del SPE mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado a través de la Subdirección de Desarrollo y Tecnología.

6. POLÍTICA DE SOFTWARE Y LICENCIAS

Todo aplicativo informático o software que usa la Entidad debe ser revisado y aprobado por la Subdirección de Desarrollo y Tecnología, en concordancia de la política de adquisición de bienes de la Unidad del SPE.

Solo está permitido el uso de software licenciado y/o aquel que sin requerir licencia sea expresamente autorizado por la Subdirección de Desarrollo y Tecnología. Las aplicaciones generadas por la Subdirección de Desarrollo y Tecnología para la Unidad del SPE en desarrollo de su misión institucional serán administradas por esta.

6.1 Control De Acceso

Los controles de acceso deberán contemplar:

- Requerimientos de seguridad de cada una de las aplicaciones.
- Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo con su perfil del cargo en la Unidad del SPE.
- Registro del personal, para el ingreso a la Unidad del SPE.

Administración de Accesos de Usuarios

Los sistemas de información de la Unidad del SPE contarán con mecanismos de control de acceso de usuarios.

Creación de Usuarios

La creación de cuentas de acceso a las aplicaciones de la Unidad del SPE se realiza en cada aplicación adicionalmente la entidad tiene administración de cuentas de dominio en el directorio activo. Los datos de acceso a los sistemas de información deberán estar compuestos por un nombre de usuario y contraseña que debe ser único por cada funcionario, contratistas o tercero.

Cuando se retire o cambie de contrato cualquier funcionario, contratista o tercero, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado y reposar el histórico de este; como también deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información, manteniendo los registros de las revisiones y hallazgos.

Administración de Contraseñas de Usuario.

Las contraseñas de acceso a la red de la Entidad deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas.

Todos los funcionarios, contratistas o terceros deberán cambiar su contraseña de acceso a la red de la Entidad con una frecuencia mínima de 3 meses.

El directorio activo deberá bloquear permanentemente al usuario luego de 5 intentos fallidos de autenticación

Normas para el uso de Contraseñas

Los funcionarios, contratistas o terceros deberán cumplir las siguientes normas para el uso de contraseñas:

- Mantener las credenciales de acceso en secreto.
- Usar contraseñas fáciles de recordar y difíciles de adivinar.
- Las contraseñas no deben estar basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
- Notificar de acuerdo con lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Equipos Desatendidos en Áreas de Usuarios.

Los funcionarios, contratistas o terceros deberán garantizar que los equipos desatendidos sean protegidos adecuadamente:

- Los equipos instalados en áreas exclusivas, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
- Bloquear el equipo de cómputo tras abandonar el puesto de trabajo. Si el usuario debe abandonar la estación de trabajo momentáneamente, activa el bloqueo de la pantalla, con el finde evitar que terceros puedan ver su trabajo.
- Las sesiones no activas en los computadores serán bloqueadas de forma automática tras inactividad superior a 5 minutos.

Control de Acceso a Internet

La Subdirección de Desarrollo y Tecnología debe bloquear al acceso de páginas de contenido para adultos, apuestas ilegales, hacking, mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por el jefe inmediato, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del encargado de seguridad de la información.

Autenticación de Usuarios para Conexiones Externas.

La autenticación de usuarios remotos deberá ser aprobada por la Subdirección de Desarrollo y Tecnología.

Control de Identificación y Autenticación de Usuarios.

Todos los funcionarios contratistas o terceros (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán nombre de usuario y contraseña, como su tarjeta de ingreso a las instalaciones de la unidad, solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

Administración de Contraseñas en el directorio activo

El directorio activo debe:

- Permitir que los usuarios cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de estas o cuando consideren que la misma ha sido comprometida.
- Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
- No permitir mostrar las contraseñas en texto claro cuando son ingresadas.

7. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SGSI DE LA UNIDAD DEL SPE

- La Unidad del SPE, garantizará la disponibilidad de sus procesos misionales y la continuidad de su operación basada en el impacto que pueden generar.
- Las credenciales de acceso a la red o recursos informáticos son carácter estrictamente personal e intransferible, los funcionarios y contratistas no deben revelar estas a terceros. Las credenciales serán suministradas por la Subdirección de Desarrollo y Tecnología a través de la mesa de ayuda.
- Los funcionarios y contratista son responsables del cambio de la clave de acceso a los sistemas de información o recursos informáticos periódicamente.
- Los funcionarios y contratistas son responsables de los registros que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.
- El acceso de un usuario a la red será suspendido a través de una solicitud enviada a la mesa de ayuda desde la Coordinación de Talento Humano en ausencia de funcionario por vacaciones, calamidad, terminación de contrato, y/o cualquier tipo de licencia, esto con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como la suplantación de identidad.
- Cuando un funcionario cesa en sus funciones o culmina la ejecución del contrato con la Unidad del SPE, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del funcionario será almacenados en medio magnéticos y entregados a la coordinación de Talento Humano para ser archivados.
- Cuando el contratista termina la ejecución del contrato con la Unidad del SPE, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información.
- Todos los funcionarios y contratistas deben respetar lo estipulado en la ley 23 de 1982 “derechos de autor” y la ley 1915 de 2018, por el cual se modifica la ley 23 de 1982 y se establecen otras disposiciones, la decisión 351 de 1993 de la comunidad andina de las naciones, así como cualquier otra que adicione, modifique o reglamente la materia.
- Integridad de la Información. Se debe proteger y garantizar que los activos de información no sufran cambios no autorizados, por lo tanto, la información debe ser protegida de modificaciones imprevistas, no autorizas, accidentales, internas o externas.
- Confidencialidad de la Información. Se debe proteger y garantizar que los activos de información, entre ellos los datos o la información sensible de la Unidad del SPE, no sean accesibles o divulgados por las personas no autorizadas.

- Disponibilidad de la Información. Se debe proteger y garantizar que los activos de información estén disponibles en todo momento, garantizando la continuidad de los servicios para el cumplimento de los objetivos misionales de la entidad.

7.1 Política De Seguridad Física y Entorno

La Secretaria General debe controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como el acceso a áreas restringidas, áreas destinadas al procesamiento o almacenamiento de la información sensible, servidores, espacios donde se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, además mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, integridad, legalidad, disponibilidad, y accesibilidad de la información.

7.2 Permanencia en las instalaciones de la Unidad del SPE.

Los funcionarios, contratistas y visitantes que se encuentren en las instalaciones físicas de la Unidad del SPE, deben estar debidamente identificados y registrados

- Los visitantes deben estar acompañados por un funcionario o contratista debidamente identificados.
- Los contratistas deben estar identificados con carné de la Unidad del SPE y ARL.

7.3 Seguridad De Las Operaciones

La Subdirección de Desarrollo y Tecnología será la encargada de la operación de los recursos tecnológicos que soportan la operación de la Unidad del SPE, así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad, legalidad, disponibilidad y accesibilidad de la información, así como asegurar que los cambios efectuados sobre los recursos tecnológicos, serán controlados y debidamente autorizados, proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Unidad del SPE, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica.

7.4 Política De Incidentes De Seguridad De La Información

la Unidad del SPE promoverá a los funcionarios y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento, así mismo asignará responsable para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo a su nivel de criticidad.

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La propiedad intelectual de la información se debe mantener, la cual se define como cualquier patente, de derecho de autor, invención o información que es propiedad de la Unidad del SPE. Todo el material que se desarrolló mientras se trabaja para La Entidad, se considera que es de su propiedad intelectual y que es de uso exclusivo de la misma, por lo tanto, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad. Así pues, Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los funcionarios, contratistas y demás colaboradores de la Unidad del SPE.

9. Plan De Seguridad y Privacidad De La Información

El siguiente plan está enmarcado en la revisión, análisis y evaluación de la documentación existente frente al Sistema de Gestión de Seguridad de la Información, ejecutando la implementación de los instrumentos para la clasificación e identificación de los activos de información de la Unidad del Servicio Público de Empleo, al igual que el instrumento para realizar la clasificación y análisis del riesgo de cada uno de los activos de información identificados por las áreas de la Entidad, en este plan tiene como pre-requisito la clasificación de activos.

Tabla 1 Plan De Seguridad y Privacidad De La Información

PLANES	ACTIVIDAD	DETALLE DE LA ACTIVIDAD	Área Responsable	Persona Responsable	EVIDENCIA O PRODUCTO	Ubicación y nombre entregable	Fechas Inicio	Fecha Fin
Plan De Seguridad y Privacidad De La Información	Evaluar y realizar ajustes al Procedimiento de inventario y clasificación de activos de Información y renombrarlo por: Procedimiento de clasificación de activos de información	Analizar y ajustar con metodología magerit	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Procedimiento de Clasificación de activos de información	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	08/02/2021	19/02/2021
	Desarrollar metodología para la clasificación de activos	Incluye: Generar procedimiento de identificación y clasificación de activos de información, Generar el instrumento para la identificación y clasificación de activos de información, Disponer el instrumento para la identificación y clasificación de activos de información, Generar la Guía para la Gestión, identificación y Clasificación de Activos de Información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Metodología para la clasificación de activos	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	22/02/2021	15/03/2021

	Aprobación metodología clasificación de activos	Aprobar la documentación: Generar procedimiento de identificación y clasificación de activos de información, Generar el instrumento para la identificación y clasificación de activos de información, Disponer el instrumento para la identificación y clasificación de activos de información, Generar la Guía para la Gestión, identificación y Clasificación de Activos de Información.	Subdirección de Desarrollo y Tecnología	Ricardo Abad Chacón Ibarra	Metodología para la clasificación de activos	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	15/03/2021	26/03/2021
	Capacitar a la Dirección General en la metodología para la clasificación de activos	Capacitar y seleccionar el responsable de actualizar el instrumento para clasificar los activos de información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Citación meet y presentación de la capacitación	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	12/04/2021	16/04/2021
	Capacitar a la Secretaria General en la metodología para la clasificación de activos	Capacitar y seleccionar el responsable de actualizar el instrumento para clasificar los activos de información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Citación meet y presentación de la capacitación	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	19/04/2021	23/04/2021
	Capacitar a la Subdirección de Administración y Seguimiento en la metodología para la clasificación de activos	Capacitar y seleccionar el responsable de actualizar el instrumento para clasificar los activos de información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Citación meet y presentación de la capacitación	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	26/04/2021	30/04/2021
	Capacitar a la Subdirección de Promoción en la metodología para la clasificación de activos	Capacitar y seleccionar el responsable de actualizar el instrumento para clasificar los activos de información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Citación meet y presentación de la capacitación	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	03/05/2021	07/05/2021
	Capacitar a la Subdirección de Desarrollo y Tecnología en la metodología para la clasificación de activos	Capacitar y seleccionar el responsable de actualizar el instrumento para clasificar los activos de información.	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Citación meet y presentación de la capacitación	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	10/05/2021	14/05/2021
	Designar al responsable de la clasificación de activos de la dependencia, concertar el alcance de	Dirección General	Dirección General	Angi Viviana Velásquez Velásquez	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021

	la clasificación de activos de la dependencia.	Planeación	Dirección General	Fredy Arturo Ramos Rincón	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Control Interno	Dirección General	Juan Manuel Bello Jaramillo	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Jurídico	Dirección General	Raúl Hernando Esteban Garcia	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Comunicaciones	Dirección General	Julian David Calderón Hortua	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Secretaría General	Secretaría General	Pablo Antonio Ordoñez Peña	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Subdirección de Administración y Seguimiento	Subdirección de Administración y Seguimiento	Fredy Arturo Ramos Rincón (E)	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Subdirección de Promoción	Subdirección de Promoción	Carlos Alberto Garzón Flórez	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
		Subdirección de Desarrollo y Tecnología	Subdirección de Desarrollo y Tecnología	Ricardo Abad Chacón Ibarra	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	18/05/2021	21/05/2021
	Realizar clasificación de activos de información por parte de Dirección General siguiendo el instrumento electrónico elaborado para dicha actividad.	Los activos de la dependencia deberán estar registrados y clasificados en el instrumento para tal fin	Dirección General	Dirección General	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	25/06/2021

	Realizar clasificación de activos de información por parte de Secretaria General siguiendo el instrumento electrónico elaborado para dicha actividad.	Los activos de la dependencia deberán estar registrados y clasificados en el instrumento para tal fin	Secretaria General	Secretaria General	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	25/06/2021
	Realizar clasificación de activos de información por parte de Subdirección de Administración y Seguimiento siguiendo el instrumento electrónico elaborado para dicha actividad.	Los activos de la dependencia deberán estar registrados y clasificados en el instrumento para tal fin	Subdirección de Administración y Seguimiento	Subdirección de Administración y Seguimiento	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	25/06/2021
	Realizar clasificación de activos de información por parte de Subdirección de Promoción siguiendo el instrumento electrónico elaborado para dicha actividad.	Los activos de la dependencia deberán estar registrados y clasificados en el instrumento para tal fin	Subdirección de Promoción	Subdirección de Promoción	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	25/06/2021
	Realizar clasificación de activos de información por parte de Subdirección de Desarrollo y Tecnología siguiendo el instrumento electrónico elaborado para dicha actividad.	Los activos de la dependencia deberán estar registrados y clasificados en el instrumento para tal fin	Subdirección de Desarrollo y Tecnología	Subdirección de Desarrollo y Tecnología	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	25/06/2021
	Revisar el instrumento de clasificación de activos.	Descargar y revisar la completitud del instrumento de clasificación de activos	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	03/06/202, 17/06/2021	03/06/202, 17/06/2021
	Enviar el avance reportado en el instrumento de clasificación de activos.	Enviar a cada subdirector el avance y el consolidado a la Dirección General	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Activos clasificados en el instrumento para tal fin	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	04/06/202, 18/06/2021	04/06/202, 18/06/2021

	Evaluar y realizar ajustes a la Política de seguridad y privacidad de la información	Analizar y ajustar, lineamientos para la Transferencia de información,	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Política de seguridad y privacidad de la información	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	11/06/2021
	Campaña de sensibilización política de seguridad de la información - PSI (3 veces al año)	Diseño Campaña	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Diseño Campaña	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	24/05/2021	04/06/2021
	Generación de Boletines o cápsulas relacionadas con Seguridad de la Información. (Dos por mes)	Diseño Cápsula	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Diseño Cápsula	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	25/01/2021	31/12/2021
	Evaluar y realizar ajustes a la encuesta de diagnóstico de seguridad y privacidad de la información	Analizar y ajustar	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Encuesta de diagnóstico de seguridad y privacidad de la información	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	22/02/2021	26/02/2021

Tabla 2 Plan de seguridad informática

PLANES	ACTIVIDAD	DETALLE DE LA ACTIVIDAD	Área Responsable	Persona Responsable	EVIDENCIA O PRODUCTO	Ubicación y nombre entregable	Fechas Inicio	Fecha Fin
Plan de seguridad informática	Evaluar y realizar ajustes al Procedimiento de Gestión de Copias de Seguridad	Analizar y ajustar con metodología	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Procedimiento de Gestión de Copias de Seguridad	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	25/10/2021	05/11/2021
	Evaluar y realizar ajustes al Procedimiento de gestión de incidentes de seguridad Informática	Analizar y ajustar con metodología	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Procedimiento de gestión de incidentes de seguridad Informática	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	02/11/2021	12/11/2021
	Evaluar y realizar los ajustes al documento Equipo de respuesta a incidentes de SI	Analizar y ajustar con metodología	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García	Documento Equipo de respuesta a incidentes de SI	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	16/11/2021	26/11/2021
	Fortalecer el acceso externo a la infraestructura tecnológica de la Entidad	VPN con doble factor de autenticación	Subdirección de Desarrollo y Tecnología	Victor Rolando Jaime Velandia	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	29/12/2019	30/06/2021
	Fortalecer la protección de la solución antivirus	Programas reunión con GMS para conocer cuáles son los productos de seguridad informática que pueden complementar la solución de kaspersky (Antivirus)	Subdirección de Desarrollo y Tecnología	Alexánder Guzmán García, Victor Rolando Jaime Velandia	Correo Electrónico	DRIVE unidad compartida: https://drive.google.com/drive/u/0/shared-drives carpeta: Seguridad de la Información	12/01/2021	13/01/2021