EMPRESA PARA LA SEGURIDAD URBANA – ESU

RESOLUCIÓN NÚMERO 098 DE 2015
(Enero 30 de 2015)

"Por medio de la cual se expide el Manual de Políticas y Estándares de Seguridad de la Información de la ESU"

El Gerente de la Empresa Para la Seguridad Urbana – ESU

En uso de las facultades legales conferidas por el Decreto Municipal 178 de 2002 y la Ley 489 de 1998, y

Considerando:

La Empresa para la Seguridad Urbana -ESU-, consciente de la importancia que representan los activos de información y teniendo en cuenta su valor en la operación y en la gestión de la Entidad como medio para alcanzar los objetivos estratégicos propuestos, y reconociendo que aunque la aparición de nuevas tecnologías representa grandes avances en el manejo de la información, también trae consigo amenazas, que de no ser detectadas oportunamente, pueden materializarse en riesgos que deberán ser mitigados, decide implementar un modelo de Gestión de Seguridad de la Información, de acuerdo con los lineamientos definidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y al Programa de Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones.

La Empresa para la Seguridad Urbana para el cumplimiento de su misión, visión, objetivos estratégicos, y apegada a sus valores corporativos, establece el Manual de Políticas y Estándares de Seguridad de la Información, con los siguientes objetivos:

Objetivo General:

Desarrollar estrategias que orienten el uso adecuado de las herramientas y recursos tecnológicos, para minimizar los riesgos a los cuales se expone la información y sacar el mayor provecho de las ventajas que ofrecen en beneficio de la entidad.

Objetivos Específicos:

- Minimizar el riesgo asociado con la seguridad de la información, en los procesos más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los lineamientos establecidos por el Departamento Administrativo de la Función Pública, en lo concerniente al Modelo Integrado de Planeación y Gestión, y al

Programa de Gobierno en Línea del Ministerio de Tecnologías de la Información y las Comunicaciones

- Apoyar la innovación tecnológica.
- Implementar el Plan de Copias de seguridad de la información.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores de la entidad, practicantes y contratistas.
- Garantizar la continuidad de los procesos de negocio frente a incidentes de la plataforma tecnológica

Este manual de políticas y estándares será de obligatorio cumplimiento por parte de quienes tengan acceso a los recursos o servicios informáticos de la ESU y se aplicará indistintamente si la entidad posee o no la propiedad de dichos recursos o servicios.

Será revisado por el comité de Gobierno en Línea anualmente con un seguimiento trimestral o cuando se identifiquen cambios significativos en el negocio que influyan en su estructura, sus objetivos o alguna condición que afecten las políticas, para asegurar que sigue siendo adecuado y ajustado a los requerimientos identificados.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1. La Empresa para la Seguridad Urbana – ESU ha establecido las siguientes Políticas Generales de Seguridad de la Información, las cuales representan la visión de la Entidad en cuanto a la protección de sus activos de Información:

2. Definir un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información, que para la ESU es el mismo comité de Gobierno en Línea.

3. Identificar y clasificar los activos de información de la ESU, para establecer los mecanismos de protección necesarios correspondientes.

4. Definir e implantar controles para proteger la información contra violaciones de autenticidad, accesos no autorizados y pérdida de integridad, que respondan a la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

5. Proteger la información a la que se acceda y procese, para evitar su pérdida, alteración, destrucción o uso indebido.

6. Realizar seguimiento y control periódico sobre el modelo de gestión de Seguridad de la Información de la ESU, para verificar su eficiencia y aplicabilidad.

7. Permitir únicamente el uso de software que haya sido adquirido legalmente por la Institución y previamente autorizado por el proceso de Tecnológica de la Información.

8. Reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que un funcionario y/o contratista identifique, a través del procedimiento establecido por la mesa de ayuda.

9. Registrar y monitorear las violaciones a las Políticas y Controles de Seguridad de la Información, y a su vez reportarlas a la Secretaría General para que dé inicio a las investigaciones pertinentes de conformidad con su competencia disciplinaria interna y a lo establecido en el Código Disciplinario Único y demás normas relacionadas.

10. Incluir este manual como parte integral del procedimiento de Inducción del Área de Gestión Humana de la Empresa para la Seguridad Urbana.

Además de las políticas generales dispuestas a cumplir en la Empresa para la Seguridad Urbana, se adoptarán las estrategias para la seguridad de la información definidas en la NTC ISO 27001:2013, y las que la Entidad ha dispuesto a partir del análisis de los riesgos de la seguridad de la Información.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN EN LA CONTRATACIÓN

Políticas:

- Identificar los riesgos asociados al acceso, procesamiento, comunicación o gestión de la información y/o la infraestructura para su procesamiento, por parte de personas o entidades externas, terceros y/o contratistas, con el fin de establecer los mecanismos de control necesarios para que la seguridad se mantenga.

- Definir una cláusula de confidencialidad de la información como parte integral en los contratos de trabajo y en los contratos con personas o entidades externas, terceros y/o contratistas, cuando deban tener acceso a la información y/o recursos de la Entidad; además, de no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información, teniendo en cuenta que cualquier violación a lo establecido en dicha cláusula será considerado como un "incidente de seguridad".

ESTRATEGIA: USO EFICIENTE DE LOS ACTIVOS DE INFORMACIÓN

Políticas:

- Los activos de información disponibles para los servidores, contratistas y/o terceros, para su uso, operación y/o custodia, de acuerdo a las funciones específicas y necesidades del trabajo a realizar son propiedad exclusiva de la ESU.

- Restringir el acceso a los documentos físicos y digitales según las normas aplicables internas y/o externas, y a los permisos determinados de acuerdo con las funciones del perfil de cargos.

- Toda la información de los procesos de la ESU, así como los activos donde ésta se almacena y se procesa están:

  - Inventariados.
  - Asignados a un responsable.
  - Protegidos y clasificados. De acuerdo con la clasificación se deben establecer los niveles de protección orientados a determinar a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación.

- Revisar la identificación y la clasificación de los activos de información anualmente y/o cuando se presenten cambios que puedan afectar las mismas.

- Todos los funcionarios y/o contratistas de la Entidad son responsables de la gestión y protección de los activos de información que se encuentren a su cargo o a los que tengan acceso; de tal forma que se mantengan los niveles de seguridad a lo largo del ciclo de vida de la información.

- El Proceso de Gestión de Tecnología de la Información es el único autorizado para la instalación de cualquier tipo de software o hardware en la Entidad, más no de la manipulación de la información que se genere dentro de los procesos.

- Asignar a cada funcionario, personal en misión, practicantes y/o contratista que ingrese a la Entidad los activos de información previa solicitud del área del proceso de Gestión del Talento Humano según el procedimiento establecido; con una anticipación de cinco (5) días hábiles, donde se especifique el nombre completo y cédula del funcionario, el tipo de equipo, aplicativos y permisos a asignar, la fecha de ingreso y su ubicación. El proceso de Gestión del Talento Humano deberá notificar con una anticipación de cinco (5) días hábiles el retiro del funcionario y/o contratista, para realizar las respectivas copias de seguridad y la desactivación del usuario.

- Entregar mediante acta a cada funcionario y/o contratista de la Entidad los activos de información asignados, donde reconozca y acepte toda responsabilidad sobre el estado de los

mismos al momento de su devolución y donde individualmente se compromete a salvaguardar y usar correctamente dichos activos.

- Definir el software y aplicaciones que se encuentran permitidas para ser instaladas en las estaciones de trabajo de la Entidad.

- Realizar seguimiento y control anualmente al licenciamiento del software y aplicaciones de la Entidad.

- El proceso de Gestión de Tecnología de la Información, es el único autorizado para realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, conexiones de red, usuarios locales de la máquina, entre otros.

- Notificar al proceso de Gestión de Tecnología de la Información, a través del procedimiento establecido, cuando sea vaya a retirar un activo de tecnología de la entidad, especificando la fecha y hora de retiro del equipo, el tiempo que estará por fuera de las instalaciones y el lugar donde se encontrará el mismo. Esta información podrá ser corroborada con el jefe inmediato o el Director del Área correspondiente.

- Asegurar todos los equipos de la entidad contra todo riesgo, daño, pérdida o robo. Ante cualquier incidente de dicha naturaleza el funcionario informará inmediatamente al proceso de Gestión de Tecnología de la Información, a través del procedimiento establecido, especificando el tipo, modo, tiempo y lugar del incidente para iniciar lo establecido en la política de activos de la entidad.

- Proteger adecuadamente todos los equipos que hacen parte de la infraestructura tecnológica de la ESU para prevenir la pérdida, el daño, el robo o los accesos no autorizados; y ubicarlos alejados de sitios que puedan tener amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética, vandalismo, entre otros.

- Los equipos de Cómputo Fijos que se asignen a cada uno de los funcionarios y/o contratistas de la entidad, sólo podrán ser reubicados por el proceso de Gestión de Tecnología de la Información o Gestión de Infraestructura.

- Evitar fumar, beber o consumir algún tipo de alimento cerca de los equipos que componen la infraestructura tecnológica de la ESU.

ESTRATEGIA: CONTROL PERMANENTE SEGÚN LAS FUNCIONES DE LOS PERFILES

Políticas:

- Definir los roles y responsabilidades, frente al nivel de acceso y los privilegios de los funcionarios que tengan acceso a la infraestructura tecnológica y a los sistemas de información de la Empresa, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la entidad.

- Implementar reglas de control de acceso para todos los sistemas de disponibilidad crítica o media de la Entidad, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

- Establecer controles duales sobre el nivel de súper usuario de los sistemas de información, de tal forma que exista supervisión a las actividades realizadas por el administrador del sistema.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN EN LAS REDES CORPORATIVAS

Políticas:

- Separar la red en segmentos físicos y lógicos para independizar la red de usuarios de conexiones con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El proceso de Gestión de Tecnología de la Información es el encargado de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

- Establecer mecanismos de identificación automática de los equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la Entidad.

- Garantizar que los puertos físicos y lógicos de diagnóstico y configuración de los equipos que soportan los sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

- Conectar a la red inalámbrica corporativa de la Entidad únicamente los equipos de cómputo asignados a los funcionarios y/o contratistas desde el proceso de Gestión de Tecnología de la Información, por consiguiente está prohibido conectar cualquier dispositivo móvil.

- Solicitar al proceso de Gestión de Tecnología de la Información, el establecimiento de una conexión a la infraestructura tecnológica de la ESU para los terceros que así lo requieran; esta solo se realizará a través de la red Inalámbrica de Invitados y será válida por 4 horas máximo.

- Prohibir a los funcionarios y/o terceros la conexión a la red LAN o WLAN de cualquier equipo por fuera del dominio esu.com.co.

ESTRATEGIA: CONTROL EFICIENTE EN EL ACCESO FÍSICO Y LÓGICO

Políticas:

- Asignar el acceso a los recursos de información de la Entidad de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se establezcan en el manual de perfil de cargos de la Entidad, así como las normas legales o leyes de protección de acceso a la información aplicables.

- Establecer medidas de control de acceso físico en el perímetro que puedan ser auditadas, así como procedimientos de seguridad que permitan proteger la información, el software y el hardware de daños intencionales o accidentales para 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.

- Contar con mecanismos que permitan monitorear y garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones en los centros de cómputo, cableado y cuartos técnicos de las oficinas.

- Utilizar siempre cifrado de datos para las conexiones remotas a la infraestructura tecnológica de la entidad, las cuales serán otorgadas por el proceso de Gestión de Tecnología de la Información, de acuerdo con las necesidades de cada usuario y previa autorización del Director del área correspondiente; será responsabilidad de cada usuario velar por la seguridad, confidencialidad e integridad de la información a la que tiene acceso de forma remota.

ESTRATEGIA: USO EFICIENTE DEL CORREO ELECTRÓNICO Y DE LAS HERRAMIENTAS DE COLABORACIÓN

Políticas:

- Usar la cuenta de correo electrónico asignada únicamente para el desempeño de las funciones dentro de la entidad.

- Los mensajes y la información contenida en las cuentas de correo (entendiéndose por esto el buzón y demás aplicativos de colaboración) son propiedad de la Entidad, y cada usuario como responsable de su buzón, debe mantener solamente información relacionada con el desarrollo de sus funciones.

- El tamaño de los buzones de correo electrónico es de 30 Gb; si un usuario requiere espacio adicional, deberá solicitarlo al proceso de Gestión de Tecnología de la Información, quien tendrá potestad para determinar o no, la viabilidad de la solicitud.

- Solo se podrán enviar y/o recibir correos electrónicos que tengan un peso máximo de 25 Mb.

- Compartir información por el aplicativo Google Drive, únicamente con usuarios internos de la Entidad; en caso de requerir compartir archivos con usuarios externos deberá ser autorizado por el Proceso de Gestión de Tecnología de la Información.

- Las conversaciones por el Chat corporativo Gtalk o Hangouts con terceros externos a la entidad sólo están permitidas para el desarrollo de las funciones propias del cargo; teniendo en cuenta que es una herramienta para facilitar la comunicación es obligatorio estar siempre conectado y en modo visible mientras se esté en el ejercicio de sus funciones.

- Enviar la información corporativa exclusivamente desde la cuenta de correo que la ESU proporciona.

- Para enviar mensajes publicitarios corporativos el proceso de Gestión de Tecnología de la Información es el autorizado para aprobar la solicitud presentada por el proceso de Gestión de la Comunicación; con el fin de evitar posibles bloqueos o inclusiones en listas negras.

- Incluir en los mensajes publicitarios corporativos enviados a terceros por medio del correo electrónico, un mensaje que le indique al destinatario como ser eliminado de la lista de distribución.

- Todos los Grupos de Distribución serán creados y configurados por el Proceso de Gestión de Tecnología de la Información, previa solicitud del proceso de Gestión de la Comunicación.

- Toda información de la ESU generada con los diferentes programas computacionales (Ej. Office, Project, Access, Wordpad, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

- Todas las firmas predeterminadas y los pie de página de los correos electrónicos, serán configurados por el Proceso de Gestión de Tecnología de la Información, previa solicitud del proceso de Gestión de la Comunicación.

- No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y/o la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Entidad; de igual forma mensajes malintencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de la ESU como punto de contacto en comunidades interactivas de contacto social, tales como facebook y/o Twitter o cualquier otro sitio que no tenga que ver con las actividades laborales.

- Enviar archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- Enviar y/o recibir archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por el Proceso de Gestión de Tecnología de la Información.

- Entregar la lista de correo electrónico de los funcionarios de la Entidad, a usuarios externos que la utilicen para fines comerciales o políticos.

- Abrir correos electrónicos de remitentes desconocidos o que sean sospechosos de tener contenido malintencionado como virus o malware.

- Intercambiar información no autorizada de propiedad de la ESU, de sus clientes y/o de sus funcionarios, con terceros.

ESTRATEGIA: ACCESO A INTERNET

Políticas:

- Controlar, verificar y monitorear la información, el uso y la navegación en internet de todos los usuarios tanto funcionarios como invitados o terceros que se conecten a la red de la entidad para navegar en internet de manera permanente, con el fin de garantizar el uso eficiente del canal corporativo y mantener la seguridad de la información.

- Realizar monitoreo permanente de los tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

- Dar un uso adecuado a este recurso y en ningún momento usarlo para realizar prácticas ilícitas o malintencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

- No está permitido:

  - Acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética, las leyes vigentes o políticas establecidas en el presente manual.

  - Acceder y usar servicios interactivos o mensajería instantánea como Facebook, Instagram, MSN Messenger, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la ESU.

  - Descarga, usar, intercambiar y/o instalar juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, archivos ejecutables, información y/o productos que de alguna forma atenten contra la propiedad intelectual, a su vez, herramientas que comprometan la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la Entidad.

  - Descargar, instalar, compartir o usar información audiovisual (videos e imágenes) utilizando sitios publicos en Internet. De requerirse esta situación, el proceso de Gestión de Tecnología de la Información, o a quienes ellos deleguen de forma explícita para esta función, deben autorizarlo asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

  - Asumir en nombre de la ESU, posiciones personales en encuestas de opinión, foros u otros medios similares por ningún funcionario y/o tercero, al igual que los empleados o subcontratistas de estos.

ESTRATEGIA: PROTECCIÓN PERMANENTE CONTRA SOFTWARE MALICIOSO

Políticas:

- Proteger todos los recursos informáticos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brinden protección contra código malicioso y prevenir el ingreso del mismo a la red de la Entidad.

- Contar con controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código móvil y malicioso. Será responsabilidad del proceso de Gestión de Tecnología de la Información autorizar el uso de las herramientas y asegurar que estas y el software de

seguridad no sean deshabilitados bajo ninguna circunstancia, así como de su actualización permanente.

- Asegurar que el análisis de seguridad y desinfección por medio del antivirus sea ejecutado a todos los dispositivos de almacenamiento una vez estos sean conectados al equipo.

- No está permitido:

  - Desinstalar y/o desactivar el software y/o herramientas de seguridad avaladas previamente por la ESU.

  - Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

  - Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

  - Usar código móvil que no haya sido debidamente autorizado por el proceso de Gestión de Tecnología de la Información.

ESTRATEGIA: GESTIÓN EFECTIVA DE LAS COPIAS DE SEGURIDAD

Políticas:

- Asegurar que la información con cierto nivel de clasificación, contenida en la plataforma tecnológica de la Entidad, como servidores, dispositivos de red para almacenamiento, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad.

- Mantener un plan de restauración de copias de seguridad y revisarlo periódicamente, con el fin de asegurar que las copias sean confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

- Establecer procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación de los respaldos.

- Definir conjuntamente con la Alta Gerencia y de acuerdo a lo determinado por la ley, los periodos de retención de las copias de seguridad y disponer de los recursos necesarios para identificar los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, permitiendo un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Almacenar en un sitio externo los medios magnéticos que contienen las copias de seguridad de la Entidad; Dicho sitio debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiada.

- Respaldar diariamente la información que se encuentre en las carpetas Mis Documentos, Mis Imágenes, o en el Escritorio de los usuarios que tengan asignados recursos virtualizados. Toda información almacenada en una ubicación diferente no será respaldada.

- Respaldar diariamente la información de la carpeta "RESPALDO" creada por el Proceso de Gestión de Tecnología de la Información, en el Escritorio de los usuarios que tienen equipos portátiles o PCs. Es responsabilidad de cada usuario almacenar la información crítica y de vital importancia en dicha carpeta, teniendo en cuenta que la información por fuera de esta carpeta no será respaldada.

- Respaldar mensualmente la información de los dispositivos móviles corporativos.

- Eliminar la información alojada en los servidores que no tenga relación con la ejecución de los procesos de la Entidad.

- Excluir del proceso de respaldo los archivos con extensiones .exe, .mp3.

ESTRATEGIA: SEGURIDAD DE LA INFORMACIÓN PARA LOS MEDIOS EXTRAÍBLES.

Políticas:

- Autorizar el uso de medios de almacenamiento removibles (CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sólo a aquellos funcionarios cuyo perfil del cargo y funciones así lo requieran, previa comunicación escrita del Director del Área correspondiente al proceso de Gestión de Tecnología de la Información.

- Implementar los controles necesarios para asegurar que en los sistemas de información de la Entidad sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento extraíbles.

- Asegurar física y lógicamente los dispositivos extraíbles con el fin de no poner en riesgo la información de la ESU contenida en los mismos.

ESTRATEGIA: USO EFECTIVO DE LAS CONTRASEÑAS DE USUARIO ASIGNADAS.

Políticas:

- Todo funcionario o tercero que requiera acceso a los sistemas de información de la ESU debe contar con un usuario (ID) y contraseña (password) asignado por el proceso de Gestión de Tecnología de la Información. El funcionario será responsable por el buen uso de las credenciales de acceso asignadas y el cumplimiento de las políticas descritas en este manual.

- Las contraseñas de acceso a los diferentes sistemas de información, no deben compartirse o revelarse a otros personas y/o usuarios; el hacerlo expone al usuario a las consecuencias disciplinarias y/o judiciales, por las acciones que los otros hagan con la misma.

- Cambiar la contraseña cada mes cumpliendo con las condiciones mínimas de longitud y complejidad establecidas por el proceso de Gestión de Tecnología de la Información.

ESTRATEGIA: SEGURIDAD PERMANENTE DEL USUARIO

Políticas:

- Mantener la información restringida o confidencial bajo llave o bloqueada con contraseña, en todo momento, en especial cuando el puesto de trabajo se encuentra desatendido, al igual que en las horas no laborales, con el fin de evitar pérdidas, daños o accesos no autorizados a la información. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general.

- Recoger de forma inmediata la información sensible que se envía a las impresoras.

- Bloquear la sesión del equipo de cómputo en el momento en que se retire del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Al finalizar las actividades, se deben cerrar todas las aplicaciones y desconectar la sesión de trabajo.

- Usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

ESTRATEGIA: EVALUACIÓN PERMANENTE DE REQUERIMIENTOS DE SEGURIDAD PARA ACTIVOS Y SOFTWARE

Políticas:

- Identificar, analizar, documentar y aprobar los requerimientos de seguridad de la información para la inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, cambios y/o actualizaciones a los sistemas existentes en la ESU, labor que debe ser responsabilidad del proceso de Gestión de Tecnología de la Información y de la dependencia que solicite el sistema en cuestión.

- Incluir en los acuerdos contractuales que se realicen entre la ESU y cualquier proveedor de productos y/o servicios asociados a Tecnología de la Información, los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor.

- Garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con la Secretaria General establecer estos aspectos en las obligaciones contractuales específicas.

ESTRATEGIA: INTERCAMBIO SEGURO DE INFORMACIÓN

Políticas:

- Firmar acuerdos de confidencialidad con los funcionarios, clientes, proveedores y/o terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio seguro por cada una de las partes y se deberán firmar previamente al acceso o uso de dicha información.

- Proteger la confidencialidad e integridad de la información, teniendo especial cuidado en el uso de los diferentes medios para el intercambio de esta, que puedan generar una divulgación o modificación no autorizada.

- Para el registro de cualquier tipo de información en las bases de datos de la plataforma tecnológica de la entidad, será requisito autorizar expresamente el tratamiento de la información por parte del titular de la misma, de conformidad con la normatividad para la protección de los datos personales. En todo caso el titular de dicha información podrá solicitar su no divulgación o tratamiento por parte de la entidad, removiéndose de las bases de datos de la ESU.

ESTRATEGIA: USO EFICIENTE DE LA TELEFONÍA

Políticas:

- Realizar seguimiento y control riguroso de forma mensual frente al consumo telefónico desde las distintas extensiones habilitadas. El uso del servicio telefónico está reservado para asuntos institucionales bajo los principios de racionalidad y austeridad del gasto público.

- En términos de tiempo, las llamadas salientes y entrantes no tendrán restricción para ningún usuario.

- En términos de destino las llamadas salientes tendrán las siguientes restricciones:

  - Llamadas internacionales: Limitadas al Gerente, Secretario General y Directores.
  - Llamadas nacionales y celulares: Limitadas al Gerente, Secretario General y Directores.
  - Llamadas locales: Habilitadas para todas las extensiones.

- Las llamadas nacionales, internacionales y celulares para otros usuarios, sólo se habilitarán previa solicitud del Director del área correspondiente al proceso de Gestión de Tecnología de la Información, justificando la razón y especificando el periodo de tiempo en que se deberá habilitar.

La presente resolución rige a partir de la fecha de expedición y deroga expresamente la resolución 109 de Abril 30 de 2013 y las demás disposiciones que le sean contrarias.

Dada en Medellín a los treinta (30) días del mes de Enero de dos mil quince (2015).

CUMPLASE

MANUEL RICARDO SALGADO PINZÓN
Gerente

Aprobó: David Andres Ospina Saldarriaga - Secretario General
Revisó: Emiro Carlos Valdez - Abogado Especialista.
Proyectó: Juliana Bermúdez Henao - Profesional Infraestructura Tecnológica