SEGURIDAD DE LA INFORMACIÓN, SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS

1.1. CONTROL DE ACCESO

• El presidente, vicepresidentes, jefes de oficina, gerentes o asesores deben solicitar y autorizar la creación, modificación, activación e inactivación, de usuarios, roles, perfiles y permisos para el acceso a la información, a los sistemas de información y a los servicios tecnológicos disponibles a través de la mesa de servicio y de los instructivos establecidos en el proceso de gestión de TICS.

• El presidente, vicepresidentes, jefes de oficina, gerentes o asesores deben y son responsables de informar por medio de la mesa de servicio los cambios de roles o responsabilidades de los trabajadores a cargo para realizar el retiro o activación de los roles, usuarios y permisos para controlar y asegurar que el acceso y privilegios establecidos a la información , los sistemas de información y servicios tecnológicos están de acuerdo a las funciones y responsabilidades asignadas a los trabajadores.

• La Gerencia Administrativa debe y es responsable de reportar las novedades de administración de personal como ingresos, egresos, vacaciones, licencias maternidad/paternidad, licencias No remuneradas superiores a 3 días e incapacidades superiores a 3 días.

• La Oficina de Tecnología de la Información debe realizar por lo menos una vez al año procesos de revisión, validación y depuración de los usuarios y de los accesos y privilegios a la información, los sistemas de información y servicios tecnológicos.

• La Oficina de Tecnología de la Información (OTI) debe realizar el control, custodia y cambio de contraseñas de los usuarios técnicos privilegiados tales como bases de datos, sistemas operativos, consolas técnicas, elementos de red y cualquier sistema tecnológico a cargo de ella. Estos usuarios y sus contraseñas (cada vez que cambien), deben ser entregados al jefe de la OTI en un sobre sellado para su custodia y uso en caso de requerirse. De la misma forma, la custodia de las contraseñas (cada vez que cambien), de los usuarios funcionales administradores de los sistemas de información tales como Orfeo, Isolucion, Neon, Sara, redes sociales, etc. a cargo de las áreas, deben ser entregados al jefe del área respectiva en un sobre sellado para su custodia y uso en caso de requerirse.

• Los trabajadores de la empresa deben seguir las políticas para la selección y uso de las contraseñas de acceso a los sistemas de información y servicios tecnológicos dispuestos y son los responsables por su custodia y por cualquier acción que se realice utilizando la cuenta de usuario y contraseña que le sea asignada.

• Las contraseñas asignadas para los servicios de tecnología por primera vez deberán ser cambiadas y posteriormente cada 30 días.

• La contraseña debe ser de mínimo 8 caracteres de longitud y debe contener dígitos, mayúscula, minúsculas, números y un carácter especial. En lo posible se debe evitar usar información personal como nombres de familiares, hijos, mascotas y fechas especiales.

• El número de intentos erróneos para el bloqueo de cuentas es de (5 intentos). Los usuarios podrán reintentar ingresar automáticamente después de 5 minutos, para lo cual el contador de intentos fallidos se reinicia en cero.

• Cualquier usuario interno o externo que requiera acceso remoto a la red y a la Infraestructura de procesamiento de Coljuegos, sea por Internet, acceso telefónico o por otro medio, siempre estará autenticado y sus conexiones deberán utilizar cifrado fuerte. Estos accesos deberán previamente estar autorizados por el presidente, jefes de oficina, vicepresidentes, gerentes o asesores, lo cual se solicitará a través del software de mesa de servicio en la cual se debe anexar la autorización.

1.2. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y DATOS SENSIBLES

• La Oficina de Tecnología de la Información debe liderar las acciones para coordinar y consolidar la identificación, clasificación y consolidación de los activos de información y datos sensibles que se gestionen en todos los procesos.

• Los líderes de los procesos, como dueños de la información, deben realizar la identificación y clasificación de los activos de información y datos sensibles, cumpliendo con el instructivo revisión activos de información y datos sensibles.

• Los líderes de los procesos, como dueños de la información, deben reportar a la Oficina de Tecnología de la Información los formatos de identificación y clasificación de activos y tendrán en cuenta la información de datos personales en los activos y datos sensibles para implementar controles para dar cumplimiento a la ley de protección de datos y a la Oficina de Tecnología de la Información para reportar las bases con datos personales a la entidad competente.

1.3. USO Y GESTIÓN DE CAMBIOS EN INFORMACIÓN

• En ningún caso, los trabajadores de la Oficina de Tecnología de la Información, podrá adicionar, modificar, eliminar y/o actualizar campos reportados como activos de información de las bases de datos y/o aplicaciones, sin la autorización escrita del presidente, vicepresidentes, jefes de oficina, gerentes o asesores (dueños de la información), cumpliendo los lineamientos del

instructivo de modificación de datos.

• La información almacenada en los equipos de cómputo de Coljuegos es de propiedad de la Entidad y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. Esto se logra mediante las siguientes actividades: asignando contraseñas no fáciles de identificar, no revelando sus contraseñas, utilizando mecanismos de identificación de roles y usuarios a los sistemas de información.

• No se permitirá la realización de actividades tales como borrar, alterar o eliminar de manera mal intencionada información de Coljuegos que se encuentre en los sistemas de información, por parte de los trabajadores oficiales y contratistas, para lograr lo anterior, se utilizarán roles y perfiles por cada uno de los sistemas.

1.4. GESTIÓN DE MEDIOS REMOVIBLES Y ALMACENAMIENTO EN LA NUBE

• El presidente, los vicepresidentes, jefes de oficina, gerentes y asesores, tendrán habilitados los puertos USB, las unidades de CD y/o DVD y el almacenamiento en la nube que disponga la Oficina de Tecnología de la Información para la gestión y transporte de los datos, documentos e información que requieran para el desarrollo de sus responsabilidades.

• Los vicepresidentes, gerentes, asesores o jefes de oficina son los responsables de solicitar y autorizar por la mesa de servicio el acceso y uso de los puertos USB o unidades de CD y/o DVD a los trabajadores a su cargo que por sus funciones y responsabilidades requieran el uso de estos dispositivos.

• La Oficina de Tecnología de la Información debe establecer los mecanismos y dispositivos USB destinados y autorizados por la empresa para guardar y transportar datos, documentos o información sensible de la empresa para evitar el uso de dispositivos personales.

• La Oficina de Tecnología de la Información debe establecer los mecanismos y lineamientos para el uso de los servicios tecnológicos disponibles para almacenamiento en la nube por parte de los trabajadores.

1.5. SEGURIDAD FISICA Y DEL ENTORNO

1.5.1. ZONAS SEGURAS

• Las zonas seguras que se identifican en Coljuegos son el centro de datos, los centros de cableado, el cuarto de cámaras, el archivo de gestión y el área de tesorería.

• La Gerencia Administrativa es la responsable de revisar, validar y otorgar los permisos de acceso por los medios de control disponibles al personal autorizado por presidente, vicepresidente, gerente o jefe de oficina responsable del área.

• La Gerencia Administrativa debe asegurar que las zonas seguras cuenten con los medios y mecanismos de control de acceso que solo permitan el acceso por el personal autorizado.

• Los responsables de las zonas seguras deben implementar mecanismos y medios que registren el ingreso de cualquier trabajador o tercero a estas zonas.
Para el centro de datos se contará con los siguientes mecanismos de protección y control de acceso:

- Cualquier acceso por personal externo a Coljuegos debe ser registrado de acuerdo a los instructivos y mecanismos dispuestos por la Oficina de Tecnología de la Información.

- Todos los accesos de terceros a las áreas seguras deberán ser autorizados previamente, por el grupo de infraestructura de la Oficina de Tecnología de la Información. Las actividades de limpieza en las áreas seguras (Centro de Cómputo), deberán ser controladas y supervisadas por el profesional especializado 1 (Líder de Infraestructura).

- El grupo de Infraestructura, velará para que en el centro de cómputo no se almacene material inflamable tales como cajas, plásticos, papeles, etc.

1.6. EQUIPOS ESCRITORIO E IMPRESIÓN

• Los equipos de escritorio y portátiles asignados por Coljuegos a los trabajadores no deberán ser prestados, usados o intervenidos por personas externas a la empresa.

• Los trabajadores de Coljuegos deben asegurar que cuando los equipos asignados estén desatendidos o sean desplazados a otras áreas por motivos de operación, no deben dejar su sesión de usuario abierta deben realizar el bloqueo de la sesión.

• Los trabajadores que tengan equipos portátiles asignados al momento de transportarlos fuera de la sede de la empresa serán responsables por la pérdida, hurto o daño del equipo. Los equipos portátiles deberán cumplir con los siguientes controles al ser retirados de la sede:

- No deben estar desatendidos en ningún momento.

- En caso de viaje, deben ir como equipaje de mano.

- Estar asegurados (cuando los equipos estén desatendidos o fuera de las instalaciones de Coljuegos) con una guaya de

seguridad provista por Coljuegos.

- Los puertos de transmisión y recepción “Bluetooth” deberán estar deshabilitados.

• El trabajador con un equipo portátil asignado debe y es responsable de informar del retiro de las instalaciones de Coljuegos a través de la mesa de servicio, seleccionando el servicio de “Retiro de equipos de cómputo”.

• En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a través de correo electrónico a la Oficina de Tecnología de la Información, el responsable del equipo deberá poner la denuncia ante la autoridad competente y responder por los valores a que hubiere lugar para la reposición del equipo.

1.6.1. REUTILIZACIÓN SEGURA DE EQUIPOS

• La Oficina de Tecnología de la Información, en el caso de la reasignación de un equipo o para aquellos equipos de trabajadores retirados, debe realizar una copia de respaldo de la información que se encuentre en el equipo y realizar el formateo del disco duro a bajo nivel.

• La Oficina de Tecnología de la Información debe reinstalar el sistema operativo y las aplicaciones y servicios tecnológicos de acuerdo con los requerimientos del nuevo trabajador.

1.6.2. ESCRITORIO Y PANTALLA DESPEJADA

• En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los trabajadores deberán dejar la información confidencial protegida bajo llave. Esto incluye: CD, dispositivos de almacenamiento USB y medios removibles en general.

• Los trabajadores deben bloquear su equipo de escritorio cada vez que se retiren de su sitio de trabajo y solo se podrán desbloquear con la contraseña asignada. Al finalizar sus actividades diarias, deberán apagar el equipo de cómputo de trabajo.

• Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla con las imágenes corporativas, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

• Es responsabilidad de todos los trabajadores que cuando en su escritorio se mantenga información considerada como confidencial o restringida, no se deje desatendida o disponible a usuarios no autorizados.

1.6.3. IMPRESIÓN DE DOCUMENTOS

• Los servicios tecnológicos disponibles para la impresión de documentos deben contar con los medios y mecanismos para que solo se impriman los documentos cuando el trabajador se haga presente y se identifique ante los dispositivos.

• Los trabajadores no deben dejar documentos impresos en las áreas de impresión y deberán asegurar su destrucción y disposición final en los sitios dispuestos para tal fin.

• Los trabajadores no deben reutilizar papel que contenga información confidencial o sensible de los procesos de la empresa.

1.7. SEGURIDAD DE LAS OPERACIONES

1.7.1. COPIAS DE RESPALDO

• Cada trabajador de la empresa es responsable de copiar de su equipo la información considerada sensible hacia la unidad M asignada para respaldo.

• La Oficina de Tecnología de la Información debe y es responsable de entregar a los trabajadores los medios y mecanismos para realizar las copias de seguridad de la información, datos y documentos sensibles.

• La Oficina de Tecnología de la Información es responsable de salvaguardar las copias de seguridad de los trabajadores mediante los instructivos, medios y mecanismos dispuestos para tal fin.

• Los trabajadores que laboran en el grupo de infraestructura de la Oficina de Tecnología de la Información, son los responsables de asegurar que se realicen las copias de seguridad de los servicios tecnológicos, sistemas de información y datos de acuerdo a los instructivos, medios y mecanismos dispuestos para tal fin. Periódicamente deben realizar y documentar pruebas de las copias de seguridad restauradas.

• Los profesionales especializados I de la Oficina de Tecnología de la Información deben tener y mantener actualizado el catálogo de las copias de seguridad que deben realizarse de los servicios tecnológicos y sistemas de información de la empresa con los atributos mínimos que permitan la gestión y control adecuado de las copias.

• La Oficina de Tecnología de la Información, grupo de infraestructura, realizará backups mensualmente de los logs de los servicios tecnológicos críticos (registro de auditoria y eventos).

• La información contenida en los servicios tecnológicos y equipos de cómputo de Coljuegos se respaldará de acuerdo a la

periodicidad definida por la Oficina de Tecnología de la Información en los instructivos respectivos, los medios utilizados se almacenarán en una custodia externa en la nube y utilizará las herramientas de backup disponibles.

1.7.2. USO DE LOS RECURSOS TECNOLÓGICOS

• El grupo de soporte a usuarios de la oficina de Tecnología de la información bloquearán los equipos de cómputo para que los trabajadores no realicen cambios en los equipos de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.

• Se podrán utilizar medios y mecanismos seguros de administración remota en los equipos de cómputo o servidores, solo por terceros con relación contractual o de soporte de servicios tecnológicos críticos con el debido acompañamiento de trabajadores de la Oficina de Tecnología de la Información, quienes brindarán el acceso remoto asegurando la plena identificación del tercero.

1.7.3. HERRAMIENTAS DE PROTECCIÓN

• Los profesionales especializados I de la Oficina de Tecnología de la Información, revisarán y mantendrán actualizadas las últimas versiones de firmas emitidas por los fabricantes (solución punto final, y soluciones de seguridad informática) y herramientas de protección que tiene instalada y arrendada Coljuegos.

1.7.4. GESTIÓN DE VULNERABILIDADES

• Los profesionales especializados I de la Oficina de Tecnología de la Información, revisarán y mantendrán actualizados los componentes técnicos (sistemas operativos, bases de datos, capas de aplicación, elementos de red y seguridad) que soportan los servicios tecnológicos de la entidad.

1.8. REDES Y COMUNICACIONES

• La Oficina de Tecnología de la Información debe adoptar, configurar e implementar los medios y mecanismos tecnológicos que controlen, aseguren y protejan los servicios tecnológicos, la información y los sistemas de información de ataques provenientes de internet.

• La Oficina de Tecnología de la Información debe asegurar las redes inalámbricas (WIFI) desde las cuales se conecten equipos o se usen servicios tecnológicos o se realicen transacciones financieras, y que cuenten con las mejores condiciones y estándares de seguridad para el acceso y la operación.

• La Oficina de Tecnología de la Información debe realizar las acciones tendientes para asegurar el acceso, operación y uso de las redes de comunicación LAN y WAN segmentando y controlando de las redes para mitigar el riesgo de accesos no autorizados o ataques informáticos a los servicios tecnológicos críticos.

1.8.1. USO DE INTERNET

• La Oficina de Tecnología de la Información controlará, verificará y monitoreará el uso adecuado del acceso a internet, considerando para todos los casos las restricciones definidas en las siguientes políticas:

- No se permitirá el acceso a páginas relacionadas con pornografía, drogas, alcohol, nueva era, música, videos, concursos, entre otros.

- No se permitirá la descarga, uso, intercambio e instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

- Cada trabajador con acceso a este recurso será responsable de dar un uso adecuado y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

- Los trabajadores y terceros contratados, igual que los empleados o subcontratistas de estos, no podrán asumir en nombre de Coljuegos, posiciones personales en encuestas de opinión, foros u otros medios similares.

- El acceso a Internet podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Coljuegos.

- Los accesos y uso de servicios interactivos o mensajería instantánea, redes sociales y demás podrán ser solo para acciones que tengan como objetivo crear comunidades para intercambiar información o actividades propias de Coljuegos.

- No se permitirá el intercambio no autorizado de información de propiedad de Coljuegos, de sus clientes y de sus trabajadores oficiales, con terceros.

• La Oficina de Tecnología de la Información realizará monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los trabajadores oficiales y/o contratistas. Así mismo, podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.

1.8.2. USO DEL CORREO ELECTRÓNICO

Coljuegos asigna una cuenta de correo electrónico como herramienta de trabajo para cada uno de sus trabajadores; su uso se encuentra sujeto a las siguientes políticas:

• El trabajador que tenga asignada una cuenta de correo electrónico institucional debe revisar, administrar y depurar frecuentemente su buzón para mantener sólo mensajes requeridos para soportar sus funciones y responsabilidades.

• La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de Coljuegos, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la buena imagen de la Entidad.

• El tamaño de los buzones de correo lo determinará la Oficina de Tecnología de la Información de acuerdo con las necesidades de cada usuario y servicios adquiridos con terceros.

• No se podrán enviar o reenviar 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 de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

• El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación del área encargada y deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución.

• Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por Coljuegos y deberán conservar en todos los casos el mensaje legal corporativo.

• No se permitirá el acceso a cuentas de correos personales de ningún tipo desde la red de Coljuegos y solo se podrán utilizar las cuentas de correo electrónico suministradas por Coljuegos. Algunos ejemplos de los sistemas de correo electrónico personales no autorizados son: Hotmail, Yahoo, Gmail, Terra, TV Cable, ETB, EPM, entre otros.

• La creación de correos electrónicos institucionales (aquellos asignados a un área o proceso) debe ser tramitada por el vicepresidente o jefe de oficina responsable del proceso y de la necesidad describiendo la problemática, los grupos de interés y los mensajes que circularán por la cuenta. La Oficina Asesora de Planeación en el marco del sistema de gestión de calidad y la Oficina de Tecnología de la Información como administradora del servicio autorizarán los correspondiente para la creación.

1.8.3. USO DE REDES SOCIALES

• El grupo de comunicaciones debe usar y operar las cuentas de redes sociales institucionales bajo un protocolo de seguridad y control, que asegure la confidencialidad de las claves de acceso y del manejo de contenido.

• El trabajador que realice el rol de community manager debe asegurar y realizar el cambio periódico de las contraseñas y asociar todas las cuentas a correos institucionales y no personales. Las claves actualizadas deben ser entregadas y custodiadas por el jefe directo.

• El grupo de comunicaciones y el trabajador que realice el rol de community manager debe asegurarse que la información que pública y comparte por las redes sociales debe provenir de fuentes certificadas y se debe acatar, respetar y cumplir lo establecido en la legislación y normatividad vigente sobre derechos de autor, marca registrada, derechos de publicidad y otros derechos de terceros.

1.8.4. USO DE DISPOSITIVOS MÓVILES

En caso de que se presente la pérdida o robo de un dispositivo móvil de la entidad o de uno de sus colaboradores en donde se tenga acceso al correo corporativo y/o aplicaciones de Coljuegos, el servidor público o contratista debe avisar inmediatamente a la OTI del extravío o hurto, para que en coordinación con esta dependencia, se proceda a modificar de inmediato las contraseñas de acceso y a cerrar la sesión en el dispositivo móvil, con el fin de garantizar la seguridad, integridad y confiabilidad de la información.

1.9. CONTINUIDAD DE LOS SERVICIOS TECNOLÓGICOS

La Oficina de Tecnología de la Información debe realizar anualmente la documentación, actualización y, en la medida de las posibilidades y capacidades, pruebas de los planes de contingencia de los servicios tecnológicos críticos para la operación de Coljuegos que permitan mitigar los riesgos relacionados con la interrupción de la operación de la empresa, que contemplen como mínimo:

• Identificación de los servicios tecnológicos críticos

• Identificación de componentes asociados a los servicios

• Identificación del equipo de trabajo, roles y responsabilidades de quienes lo integran, para proporcionar la continuidad de servicios tecnológicos en Coljuegos.

• Documentación y revisión de los procedimientos a seguir en caso de una contingencia para los servicios tecnológicos identificados.

• Pruebas y valoración de la ejecución de los planes de contingencia para actualizar el plan y mejorar las capacidades de reacción.

1.10. RELACIÓN CON TERCEROS

Todas las áreas de Coljuegos que tengan relación y contratos con terceros (empresas o personas naturales), donde compartan información sensible, deberán firmar acuerdos de confidencialidad y definir controles que permitan minimizar riesgos sobre la confidencialidad, integridad y disponibilidad de la información.

1.11. GESTIÓN DE INCIDENTES DE SEGURIDAD

La Oficina de Tecnología de la Información, tendrá en operación una herramienta de auditoria que generará alertas cuando se presenten alteraciones sobre los datos sensibles de la entidad.

• Los dueños de la información y líderes de proceso serán los responsables de revisar, analizar las alertas que generarán la herramienta de auditoria.

• Los dueños de la información y líderes de proceso serán los responsables de convocar el grupo de manejo de crisis/incidentes que permita evaluar y definir el manejo del evento identificado.

• El grupo de manejo de crisis/incidentes analizarán las implicaciones, impacto que podría generar la afectación de la disponibilidad, integridad o disponibilidad de la información, y se definirán los planes de tratamiento, y comunicación a las partes interesadas de la entidad.

CONTROL DE CAMBIOS					
VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO			
		Capítulo	Párrafo / Tabla / Figura / Nota	Adición (A) o Suspensión (S)	Texto Modificado
2	09/Abr/2019	TODOS	TODOS	A/S	Se realizó cambio global a la política de seguridad de la información.
3	26/Sep/2019	1.7.1	1,3 y 5	A/S	Se realizó cambio en los párrafos 1,3 y se elimino en el párrafo 5 a la política de seguridad de la información.
3	26/Sep/2019	1.7.2	1	A/S	Se realizó cambio en los párrafos 1 a la política de seguridad de la información.
3	26/Sep/2019	1.8.2	1	A/S	Se realizó cambio en los párrafos 1 a la política de seguridad de la información.
4	10/Sep/2020	1.8.4	A		Nuevo concepto USO DE DISPOSITIVOS MÓVILES

ELABORÓ	REVISÓ	APROBÓ
Fausto Merchan Guevara TECNICO 2	Rodrigo Alarcón Avila PROFESIONAL ESPECIALIZADO 1 Edgar Eduardo Romero Bohorquez Jefe Oficina	Juan Bautista Pérez Hidalgo PRESIDENTE