Coljuegos	GESTIÓN TIC´S POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	Vigencia: 22/Ene/2018
		Versión: 1
		Código: TIC-RE-09

DESCRIPCIÓN Y RELACIÓN DE CARACTERÍSTICAS Y REQUISITOS DE SEGURIDAD

MACRO PROCESO GESTIÓN DE TIC

1.1. SATISFACCIÓN REQUERIMIENTOS TIC

• La instalación de cualquier tipo de software en los equipos de cómputo de Coljuegos será responsabilidad de la oficina de TI y por tanto son los únicos autorizados para realizar esta labor.

• La oficina de TI definirá e informará a los funcionarios de Coljuegos, la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios.

• Todo software utilizado en Coljuegos, deberá contar con la licencia de uso respectiva.

1.2. DESARROLLO DE SISTEMAS DE INFORMACIÓN

• El grupo de desarrollo y mantenimiento de software de la oficina de TI, debe incluir dentro de sus sistemas de información un módulo de auditoría y control, el cual registre la trazabilidad e informe las alertas tempranas de aquellas operaciones críticas para Coljuegos.

• El grupo de desarrollo y mantenimiento de software de la oficina de TI, deberá desarrollar y documentar los planes de pruebas que permitan soportar los cambios y/o modificaciones en las aplicaciones y herramientas que soportan los servicios tecnológicos en la entidad.

• El grupo de desarrollo y mantenimiento de software de la oficina de TI, debe tener en cuenta dentro de su gestión, el estricto cumplimiento de la separación de los ambientes de desarrollo, pruebas, y producción.

• El grupo de desarrollo y mantenimiento de software de la oficina de TI, debe cumplir con los lineamientos que permitan desarrollar y cumplir con el manual de desarrollo de sistemas de información y aplicaciones para entregar software seguro.

• El grupo de desarrollo y mantenimiento de software de la oficina de TI, debe mantener controles que permitan la protección de los datos de prueba.

• Cada vez que se realicen modificaciones a las aplicaciones de negocio y herramientas, el grupo de desarrollo y mantenimiento de software de la oficina de TI, debe cumplir con los instructivos de configuración y cambios definidos en la oficina de TI de Coljuegos.

1.2. CONTROL DE ACCESO

• Se requiere autorización del presidente, los vicepresidentes, jefes de oficina, gerentes o asesores para la creación, modificación, activación e inactivación, de usuarios, roles, perfiles y permisos para el acceso a la información de los sistemas de información.

• Los accesos y privilegios asignados a los usuarios a los diferentes recursos de la plataforma tecnológica informática, deben ser previamente autorizados por los jefes de oficina, vicepresidentes, asesores o gerentes de Coljuegos a través del software de mesa de ayuda.

• Se debe por lo menos una vez al año, realizar auditorías y monitoreos a los controles implementados para la gestión de acceso y privilegios de los recursos informáticos.

• Se debe por lo menos una vez al año, hacer depuración de los usuarios, roles, perfiles y permisos para el acceso a la información de cada sistema de información.

• Se debe por lo menos una vez al año, realizar auditorías y monitoreo a los controles implementados para la gestión de acceso y privilegios asignados a los usuarios de los sistemas de información.

• Los ambientes de desarrollo y pruebas serán de control total de los grupos de desarrollo y quedarán organizados con la data que requieran, para lo cual deberán solicitar a los administradores de bases de datos, los datos necesarios para que cumplan con sus actividades.

• Los ambientes de pre-producción y producción serán de responsabilidad única y exclusiva de los profesionales especializados I (líder de infraestructura, desarrollo y soporte y mantenimiento de aplicaciones). Por ningún motivo deberán suministrar las claves de los usuarios privilegiados de sistema operativo, bases de datos y servidores de aplicaciones. Los usuarios y sus claves, deberán ser entregados cada vez que se cambie al jefe de la oficina de TI en un sobre totalmente sellado para su custodia y uso en caso de requerirse.

1.2.2. CRIPTOGRAFÍA

• En Coljuegos no se permitirá el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por el Jefe de la Oficina de TI. La administración de claves criptográficas y certificados digitales estará a cargo del Jefe de la Oficina de TI.

1.3. ENTREGAR SOPORTE

• En ningún caso, el personal de la oficina de TI, podrá adicionar, modificar, eliminar y/o actualizar datos de los sistemas de información y/o aplicaciones, sin la autorización escrita de los Jefes de Oficina o Vicepresidentes.

• El truncamiento de logs, el monitoreo y verificación del rendimiento de las bases de datos, sistemas operativos y demás software, se deberán realizar por lo menos una vez al mes. Antes de truncar los logs, éstos deben salvaguardarse.

• Se deberán registrar y monitorear los logs de auditoría de los sistemas de información, aplicaciones, bases de datos, sistemas operativos y firewall, además realizar una revisión semestral a los mismos.

1.3.1. GESTIÓN DE ACTIVOS

1.3.1.1. ACTIVOS Y DATOS SENSIBLES

• La oficina de tecnología de la información coordinará y consolidará la clasificación de los activos y datos sensibles.

• Los dueños de la información realizarán la clasificación de los activos y datos sensibles, cumpliendo con el instructivo revisión activos de información y datos sensibles.

• Los dueños de la información reportarán y tendrán en cuenta la información de datos personales en los activos y datos sensibles que les permitan implementar controles para dar cumplimiento a la ley de protección de datos.

1.3.1.2. GESTIÓN DE MEDIOS REMOVIBLES

• Sólo se habilitarán los puertos USB o unidades de CD y/o DVD, a los usuarios que autoricen los Vicepresidentes o Jefes de Oficina, lo cual se solicitará a través del software de mesa de ayuda.

1.3.2. CONTROL DE ACCESO

1.3.2.1. CONTROL DE ACCESO

• El presidente, los vicepresidentes, jefes de oficina, gerentes y asesores, tendrán habilitados los puertos USB y las unidades de CD y/o DVD.

• Los equipos que tengan habilitados la unidad de CD y/o DVD o los puertos USB, solo pueden conectar los dispositivos destinados y autorizados por la entidad, no pueden conectar ni almacenar información de la entidad en dispositivos personales.

• No se permitirá el almacenamiento y/o procesamiento de información confidencial de propiedad de Coljuegos en equipos o dispositivos de propiedad de los funcionarios o contratistas, a menos que los jefes de oficina, vicepresidencias lo autoricen formalmente.

• 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: colocando contraseñas no fáciles de identificar, no revelando sus contraseñas, utilizando mecanismos de identificación de roles y usuarios a los sistemas de información.

• Para la implementación y mantenimiento de los sistemas de información y/o aplicaciones, la oficina de TI deberá contar con tres servidores independientes para los siguientes ambientes: desarrollo, pruebas y producción.

• 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 funcionarios y contratistas, para lograr lo anterior, se utilizarán roles y perfiles por cada uno de los sistemas.

1.3.2.2. ÁREAS SEGURAS

El centro de cómputo de Coljuegos se define como un área segura y contará con los siguientes mecanismos de protección y control de acceso:

• Todos los accesos al centro de cómputo deben quedar registrados en la planilla de

control de acceso.

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

• En el centro de cómputo no se puede almacenar material inflamable tales como cajas, plásticos, papeles, etc.

1.3.2.3. POLÍTICA DE SERVICIOS DE RED

• 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 los Jefes de Oficina o Vicepresidentes, lo cual se solicitará a través del software de mesa de ayuda.

• Los usuarios deberán seguir las políticas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando la cuenta de usuario y contraseña que le sea asignada.

• Las contraseñas se deben cambiar la primera vez que se usen las cuentas asignadas y periódicamente se cambiaran según los requerimientos de la infraestructura de procesamiento de información.

• 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.

• La Vigencia máxima para el cambio de contraseñas por parte de los usuarios será de 60 días.

• El Número de intentos erróneos para el bloqueo de cuentas (9 intentos). Los usuarios podrán reintentar ingresar automáticamente después de 5 minutos, para lo cual el contador de intentos fallidos se reinicia en cero.

1.3.3. SEGURIDAD FISICA Y DEL ENTORNO
1.3.3.1. SEGURIDAD DE EQUIPOS

• Las estaciones de trabajo ya sean equipos portátiles o equipos de escritorio asignados por Coljuegos, no deberán ser prestados a personas externas a la entidad. En caso de requerirse la oficina de TI suministrará el equipo.

1.3.3.1.1. SOBRE EL USO INTERNO

• Los funcionarios de Coljuegos deben asegurar que los equipos de cómputo portátiles se mantengan con la guaya de seguridad suministrada, mientras se encuentren en su lugar de trabajo.

• Los funcionarios de Coljuegos deben asegurar que los equipos de cómputo portátiles asignados y que sean desplazados a otras áreas de la organización por motivos de operación, deben llevar la guaya respectiva, así mismo, no dejar su sesión de usuario

abierta cuando tenga que levantarse del sitio donde esté trabajando. Su mal uso es responsabilidad del usuario al cual se haya asignado.

• Es responsabilidad de funcionarios de Coljuegos, que cuando se retiren de su lugar de trabajo se realice el bloqueo de la sesión respectiva en los equipos de cómputo asignados.

1.3.3.1.2. SOBRE EL USO EXTERNO

Los equipos portátiles no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano. En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a través de correo electrónico al profesional especializado 1 (líder de soporte), el responsable del equipo deberá poner la denuncia ante la autoridad competente. Los equipos portátiles deberán cumplir con los siguientes controles:

• 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 de infrarrojo y “Bluetooth” deberán estar deshabilitados.

• Cuando un equipo de cómputo sea retirado de las instalaciones de Coljuegos, se deberá solicitar su retiro a través del software de mesa de ayuda, seleccionando el servicio de “Retiro de equipos de cómputo”, en caso de no tener la autorización del Jefe de la Oficina de TI, no se podrá retirar el equipo de la entidad.

1.3.3.1.3. REUTILIZACIÓN SEGURA DE EQUIPOS

• Cuando un equipo sea reasignado o para aquellos equipos de usuarios que se han retirado, el técnico 2 o el asistencial 2 del grupo de soporte a usuarios dentro de la oficina de tecnología, realizará una copia de respaldo de la información que se encuentre en el equipo, posteriormente formateará el disco a bajo nivel con la herramienta DBAN. Reinstalará el sistema operativo y las aplicaciones de acuerdo con los requerimientos del nuevo usuario.

1.3.3.2. POLÍTICA DE ESCRITORIO Y PANTALLA DESPEJADA

• En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar la información confidencial protegida bajo llave. Esto incluye: CD, dispositivos de almacenamiento USB y medios removibles en general. Los usuarios deberán bloquear su estación cada vez que se retiren de su sitio de trabajo y solo se podrán desbloquear con la contraseña del usuario. Al finalizar sus actividades diarias, deberán apagar la estación de trabajo.

• Todas las estaciones de trabajo deberán 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. Los usuarios deberán recoger de forma inmediata todos los documentos que envíen a las impresoras. Así mismo, no se deberá reutilizar papel que contenga información confidencial.

• 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.

1.3.4. SEGURIDAD DE LAS OPERACIONES
1.3.4.1. COPIAS DE RESPALDO

• Cada usuario de Coljuegos es responsable de copia de la información almacenada en su PC, en la unidad lógica definida asignada por la oficina TIC.

• El grupo de soporte de la oficina de TI es responsable de salvaguardar la información residente en la unidad lógica definida en cada uno de los pc de los usuarios y realizará los backups diarios.

• La oficina de TI, grupo de infraestructura, realizará backups mensualmente de los logs de los sistemas (registro de auditoria y eventos) respectivos.

• Los profesionales especializados I (líder de infraestructura y líder de soporte primer nivel), son los responsables de realizar en horario que no interfiera con las operaciones normales de Coljuegos los backups a las bases de datos, sistemas de información y aplicaciones.

• Los profesionales especializados I, mantendrán actualizado el catálogo de los Backups realizados a las bases de datos, sistemas de información, aplicaciones e información de los funcionarios de Coljuegos.

• Los profesionales especializados I (líder de infraestructura y líder de soporte primer nivel), están encargados de garantizar el resultado de las copias de seguridad y para lo anterior se compromete a realizar pruebas a las copias de seguridad ejecutadas.

• La información contenida en los servidores y computadores de Coljuegos se respaldará de forma diaria, los medios utilizados se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico.

1.3.4.2. USO DE LOS RECURSOS TECNOLÓGICOS

• Los usuarios no deben realizar cambios en las estaciones 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. Estos cambios podrán ser realizados únicamente por la oficina de TI.

• No se permitirá la administración remota de ningún dispositivo, equipo o servidor de la infraestructura de procesamiento de información de Coljuegos sin la previa autorización del jefe de la oficina de TI.

1.3.4.2. HERRAMIENTAS DE PROTECCIÓN

• Los profesionales especializados I de la oficina de TI, 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.

1.3.4.3. GESTIÓN DE VULNERABILIDADES

• Los profesionales especializados I de la oficina de TI, 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.

1.3.5. SEGURIDAD DE LAS COMUNICACIONES

1.3.5.1.1. USO DE INTERNET

La oficina de TI controlará, verificará y monitoreará el uso adecuado de este recurso, 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.

• No se permitirá el intercambio no autorizado de información de propiedad de Coljuegos, de sus clientes y de sus funcionarios, con terceros.

• La oficina de TI realizará monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o contratistas. Así mismo, podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación.

• Cada uno de los usuarios será responsable de dar un uso adecuado de internet 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 funcionarios y contratistas, al 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.

• 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.

• No se permitirá el acceso ni el uso de servicios interactivos o mensajería instantánea como ICQ, NetMeeting, Kazaa, Chat, MSN Messenger, Yahoo, Skype, Net2phone, facebook y otros similares, que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias de Coljuegos.

1.3.5.1.2. USO DEL CORREO ELECTRÓNICO

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

• 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.

• Los mensajes y la información contenida en los buzones de correo son de propiedad de Coljuegos y cada usuario, como responsable de su buzón, deberá mantener los mensajes de los últimos seis (6) meses relacionados con el desarrollo de sus funciones, es decir, que no deberá borrar información de Coljuegos que haya sido enviada o recibida en los últimos seis (6) meses.

• El tamaño de los buzones de correo lo determinará la oficina de TI de acuerdo con las necesidades de cada usuario.

• No se permitirá enviar o recibir mensajes con un tamaño superior a diez (10) Mb a dominios externos y máximo veinticinco (25 Mb) a correos internos. De igual forma, 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.

1.3.6. CONTINUIDAD DE LA INFRAESTRUCTURA y SERVICIOS TECNOLÓGICOS

• El jefe de la oficina de TI, en su plan de gestión anual, debe tener la actividad relacionada con la elaboración e implantación del plan integral de contingencia informático, que permita reaccionar ante eventos no esperados; ya sea por efectos de la naturaleza o por actos humanos (robo, sabotaje, terremoto, incendio, inundación, cambio inesperado de las instalaciones de Coljuegos, entre otros).

• El jefe de la oficina de TI, en su plan de gestión anual, debe tener la actividad relacionada con el equipo de trabajo, roles y responsabilidades de quienes lo integran, para proporcionar la continuidad de servicios tecnológicos en Coljuegos.

• El jefe de la oficina de TI, en su plan de gestión anual, debe tener las actividades relacionadas con la elaboración de los procedimientos a seguir en caso de una contingencia para los servicios tecnológicos.

• Se deberá probar el plan de contingencia informático por lo menos una vez cada año y con base al resultado de las pruebas y simulaciones se actualizará el plan.

1.3.8. 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.

1.3.9. GESTIÓN DE INCIDENTES DE SEGURIDAD

• La oficina de TI, 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 definiran 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
1	04/Ene/2018	NA	NA	A	Primera versión del documento, producto de la división de las políticas de TI con las políticas de seguridad de la información.

ELABORÓ	REVISÓ	APROBÓ
Elizabeth Hernandez PROFESIONAL 0	Luis Alfredo Mendoza Lozano PROFESIONAL 1 Sergio Andres Soler Rosas JEFE DE OFICINA TIC Omar Fernando Mendez Soto PROFESIONAL ESPECIALIZADO 1 (E)	Juan B. Perez Hidalgo PRESIDENTE