TABLA DE CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos de la Política de Seguridad y Privacidad de la Información son derechos reservados por parte del Instituto Municipal de Cultura, Recreación y Deporte de Zipaquirá - IMCRDZ, a través de la Estrategia desarrollada por Gobierno en línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013, así como a los anexos son derechos reservados por parte de ISO/ICONTEC.

2. INTRODUCCIÓN

Actualmente, la seguridad de la información ha tomado gran auge, dadas las condiciones cambiantes y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

La información es considerada actualmente como el activo más importante de las instituciones, es por ello que se debe tener muy presente cómo protegerla de todo tipo de ataques que le puedan hacer; bien sea ataques físicos o lógicos. Por esta razón es muy importante tener bien definidas políticas que permitan darle protección al sistema de información.

La norma comprende las siguientes 10 áreas: Política de seguridad, Control de acceso a los sistemas, Administración de los equipos y las operaciones, Desarrollo y mantenimiento de los sistemas, Seguridad física y del entorno, Cumplimiento, Seguridad del personal, Organización de la seguridad, Clasificación y control de los activos, y Administración para la continuidad de las empresas. Aunque esta norma no es homologable constituye una referencia obligatoria en materia de seguridad de la información sobre la cual nos debemos guiar, este documento adicionalmente, está elaborado de acuerdo a los lineamientos establecidos en el Manual de Políticas Generales de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones.

Con el ánimo de establecer la política de Seguridad de la Información, este documento define unos lineamientos para la gestión de la seguridad en la entidad, asegurar la protección de la información minimizando los posibles riesgos a los cuales se puede ver avocada la entidad.

En Colombia la Comisión Intersectorial de Políticas y Gestión de la Información para la Administración Pública recomienda la implementación de políticas de seguridad de la información para optimizar la seguridad de los sistemas de información a través de los estándares internacionales, apoyándose fundamentalmente en el ISO/IEC 17799:2005.

Las políticas de seguridad de la información son una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización. Estas

conforman el conjunto de lineamientos que una institución debe seguir para asegurar la confiabilidad de sus sistemas. En razón a lo anterior, son parte del engranaje del sistema de seguridad que la organización posee para salvaguardar sus activos.

Las políticas se elaboran con el fin de que tengan aplicación a largo plazo y guíen el desarrollo de reglas y criterios más específicos que abordan situaciones concretas. Las políticas son desplegadas y soportadas por estándares, mejores prácticas, procedimientos y guías. Las políticas son de carácter obligatorio y la incapacidad o imposibilidad para cumplir una política exige que se apruebe una excepción.

3. OBJETIVO GENERAL

Proteger, preservar y administrar objetivamente la información del IMCRDZ junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

4. ALCANCE

Las Políticas de Seguridad de la Información constituyen la posición oficial de la entidad en relación con la seguridad de la infraestructura y sistemas informáticos del IMCRDZ. Su cumplimiento por parte de los usuarios de los servicios informáticos del IMCRDZ es de carácter obligatorio. En ellas se ofrece de forma respetuosa, cortés y con responsabilidad, los lineamientos en materia de seguridad de la información con el fin de garantizar el buen funcionamiento del área.

Todas las personas que hagan uso de los servicios informáticos del IMCRDZ deberán conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no exonera a la persona de las responsabilidades asignadas.

Éstas políticas de seguridad de la información están dirigidas a todos los usuarios internos y externos que utilicen los servicios de la plataforma tecnológica del IMCRDZ.

5. GESTIÓN DE EQUIPOS

5.1 INSTALACIÓN DE EQUIPOS DE CÓMPUTO

El Almacén deberá llevar un registro de todos los equipos de cómputo propiedad del IMCRDZ.

Todo equipo de cómputo (computadores, celulares, computadores portátiles, y otros accesorios), que esté o sea conectado a la Red de datos del IMCRDZ, ya sea física o por red inalámbrica, o aquel que en forma autónoma se tenga y que sea propiedad de la entidad debe sujetarse a las normas y procedimientos de instalación que emite TIC.

Cada equipo debe tener un propósito específico y una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos que TIC tiene establecido en su normatividad de este tipo como: seguridad física, condiciones ambientales, alimentación eléctrica, control de acceso.

Los responsables de las distintas áreas conjuntamente con el área de sistemas deberán dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en la ubicación o adjudicación de equipos de cómputo. Previo a la reasignación de alguno de estos elementos se debe hacer el trámite respectivo ante almacén general.

La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos, en caso de que existan, al área de sistemas o TIC, y como se mencionó en el apartado anterior, al almacén general.

5.2 ASIGNACIÓN DEL EQUIPO DE CÓMPUTO.

Todo usuario del IMCRDZ al que se le asigne un equipo de cómputo (computadores, computadores portátiles, celular, y otros accesorios) propiedad del IMCRDZ será responsable de su uso y de su seguridad física.

El usuario al que se le haga entrega de equipo de cómputo deberá firmar un acta de entrega y quedará registrado en el Almacén General.

El usuario debe verificar que el equipo de cómputo entregado cuente con todas las herramientas necesarias para su labor diaria (Sistema de información, Antivirus, Procesador de texto, etc.).

5.3 RESPONSABILIDADES Y CUIDADO DEL EQUIPO DE CÓMPUTO

Los usuarios no deben abrir los computadores, impresoras, reguladores de voltaje etc, para retirar o instalar partes.

Se prohíbe el consumo de alimentos en zonas cercanas al equipo de trabajo.

El equipo de cómputo no debe ser soporte de ningún elemento que atente contra su normal funcionamiento y ventilación como (carpetas, decoraciones, o cualquier otro objeto). No deben colocarse elementos como plantas, bebidas, alimentos, libros o carpetas sobre los equipos, ni bloquear las rejillas de ventilación.

Cada usuario es responsable de apagar correctamente el equipo y el monitor que está a su cargo al finalizar la jornada de trabajo.

El usuario es el encargado de asegurarse de que sus archivos cuenten con las protecciones necesarias de escritura, lectura y ejecución para los casos en que estos sean compartidos con otros usuarios.

Es responsabilidad del usuario tener la información organizada de manera correcta en una única carpeta, que puede contener otras, con el fin de realizar el respaldo (BackUp) de su información incluidos los correos electrónicos.

Los contratistas deben entregar en medio magnético la documentación producto de la labor contratada al finalizar el contrato al supervisor.

El área de sistemas o TIC´s deberán habilitar el bloqueo de pantalla automático luego de un período de inactividad de 10 minutos.

En caso de notar un mal funcionamiento en el sistema, presencia de virus, código malicioso, SPAM o algún otro problema, los usuarios deberán notificar a través de alguno de los medios de comunicación interna al responsable de sistemas o TIC´s.

Es responsabilidad del usuario realizar revisiones con el antivirus instalado en el equipo de los archivos en discos, memorias externas USB, CD, DVD, Discos duros externos. Los usuarios deberán explorar los discos antes de copiar o abrir archivos o antes de utilizarlos para iniciar el sistema.

Todos los equipos de cómputo deben contar con software antivirus instalado y actualizado.

Los usuarios deberán reportar al responsable de sistemas o TIC´s, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad del IMCRDZ.

Cada usuario debe dar a conocer al responsable de sistemas o TIC´s, la respectiva clave de su equipo de cómputo, quien la registrará en el archivo "Matriz de Inventario Tecnológico del IMCRDZ" como parte integral de la información prioritaria del equipo. De lo contrario el responsable de sistemas o TIC´s no tendrá acceso eficiente al equipo para realizar el correspondiente BackUp ni el mantenimiento preventivo.

5.4 CAMBIOS AL HARDWARE Y SOFTWARE

Los equipos de cómputo no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del responsable de sistemas o TIC´s.

La actualización o cambios de hardware en los equipos de cómputo será llevada a cabo por el responsable de sistemas o TIC´s, este proceso quedará registrado en la hoja de vida del equipo de cómputo. El usuario al cual está asignado el equipo deberá firmar una nueva acta de entrega donde se reflejan sus características, configuración y ubicación.

Todos los equipos de cómputo del IMCRDZ se encuentran relacionados en un inventario, "Matriz de Inventario Tecnológico del IMCRDZ", especificando información prioritaria, configuración y descripción de modificaciones o mantenimientos.

Queda estrictamente prohibido instalar software en los computadores sin las debidas autorizaciones. El único autorizado parar realizar instalación y desinstalación de programas, así como cambios de configuración en el sistema

operativo, es el responsable de sistemas o TIC´s. Esto con el fin de evitar malas configuraciones, deficiencias, infecciones en el sistema operativo, y para garantizar que la “Matriz de Inventario Tecnológico del IMCRDZ” permanece actualizada y vigente.

Los equipos de cómputo no deben tener instalado ningún software que no sea el licenciado y requerido para que el usuario desarrolle su trabajo.

5.5 MANTENIMIENTO DEL EQUIPO DE CÓMPUTO

Al responsable de sistemas o TIC´s, corresponde la realización del mantenimiento preventivo y correctivo de los equipos. Los mantenimientos preventivos se programarán trimestralmente en el Formato Cronograma de mantenimiento y Backup mensual- PA-FT-10-02, que será dado a conocer con una semana de anterioridad al mantenimiento.

En el caso de los equipos de cómputo cuyo mantenimiento sea atendido por terceros, el responsable de sistemas o TIC´s deberá supervisar el proceso de mantenimiento.

Por motivos de normatividad queda estrictamente prohibido dar soporte y mantenimiento a equipos de cómputo que no sean propiedad del IMCRDZ.

5.6 ACTUALIZACIÓN DEL EQUIPO DE CÓMPUTO

El responsable de sistemas o TIC´s es el encargado de gestionar que todo el equipo de cómputo (computadores, computadores portátiles y otros accesorios), que sean propiedad de EL IMCRDZ sean actualizados tanto en hardware como en software, tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

Todos los cambios tanto físicos como de software en el equipo de cómputo estarán a cargo del responsable de sistemas o TIC´s. Si el equipo de cómputo cambia de responsable se deberá notificar al responsable de sistemas o TIC´s y al Almacén general, para actualizar la hoja de vida del equipo.

Los responsables de las distintas áreas deberán dar cabal cumplimiento con las notificaciones correspondientes al responsable de sistemas o TIC´s sobre la

actualización requerida para el equipo que tenga asignado y todo aquello que implique cambios físicos o lógicos en los equipos de cómputo.

5.7 REUBICACIÓN DEL EQUIPO DE CÓMPUTO

La reubicación del equipo de cómputo se realizará por medio del responsable de sistemas o TIC´s.

El equipo de cómputo a reubicar sea del IMCRDZ o bien externo debe contar con la autorización del responsable de sistemas o TIC´s, informando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo. Así mismo se debe informar al responsable del Almacén General.

Si el área donde se va a reubicar el equipo de cómputo no cuenta con las condiciones mínimas para su funcionamiento y seguridad (punto de red, corriente regulada, seguridad física) se deberá informar al responsable de sistemas o TIC´s mínimo 15 días hábiles antes de la reubicación para verificar las condiciones y evaluar las posibles adecuaciones.

5.8 ELIMINACION SEGURA DE INFORMACIÓN EN EQUIPOS Y OTROS MEDIOS

- En todo medio informático reutilizable como equipos rentados, equipos pertenecientes al IMCRDZ, discos externos, memorias USB, entre otros, deberá realizarse un proceso de borrado seguro en la información antes de su entrega, devolución o dada de baja.

- Los documentos físicos con información confidencial que requieran ser destruidos, debe realizarse de acuerdo a los procedimientos de Gestión Documental.

6. CONTROL DE ACCESO

6.1 ACCESO A EQUIPOS DE CÓMPUTO

- Todos los equipos de cómputo del IMCRDZ deberán estar protegidos con una clave de acceso al usuario que será conocida por el funcionario a quien se le asignó dicho equipo y por el responsable de sistemas o TIC´s. Dicha clave será registrada en la Matriz de Inventario Tecnológico y se deberá mantener actualizada.

- El responsable de sistemas o TIC´s le asignará a cada usuario de la plataforma tecnológica del IMCRDZ un usuario para el acceso correspondiente. La contraseña la escogerá directamente el usuario y será confidencial, solo el usuario y el responsable de sistemas o TIC´s deben conocer la contraseña. Esta debe poseer un mínimo de 6 caracteres y deberá ser alfanumérica.

- El nombre de usuario y contraseña son responsabilidad exclusiva de cada uno de los usuarios y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal. De acuerdo con lo anterior, los usuarios no deben obtener palabras claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido, ni guardar la contraseña en scripts, macros, teclas de función de terminal, archivos de texto, o en otras ubicaciones en donde personas no autorizadas puedan usarlas.

- Todo cambio de contraseña debe reportarse al responsable de sistemas o TIC´s con el fin de mantenerla actualizada en la Matriz de Inventario Tecnológico.

- Los usuarios son responsables de todas las actividades llevadas a cabo con su cuenta de usuario y sus claves personales, tanto en el acceso a sus equipos como en el acceso a la plataforma tecnológica del IMCRDZ. Las cuentas de usuario y claves de acceso son de uso personal e intransferible.

- La vigencia de la cuenta de usuario estará determinada por el tiempo de vinculación del contratista o funcionario con EL IMCRDZ.

6.2 CONTROL DE LA INFORMACIÓN

- Los usuarios deben informar inmediatamente al responsable de sistemas o TIC´s toda vulnerabilidad encontrada en los sistemas informáticos, ya sea información interna o externa.

- Todo equipo de cómputo antes de conectarlo a la red interna del IMCRDZ, deben ser autorizadas por el responsable de sistemas o TIC´s.

- Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores de la entidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

- Los usuarios no deben suministrar cualquier información del IMCRDZ a ningún ente externo sin las autorizaciones respectivas.

- Los usuarios no deben consultar, modificar, destruir, copiar o distribuir los archivos de la entidad sin los permisos respectivos.

- Todo usuario que utilice los recursos tecnológicos y la Red del IMCRDZ, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad, confiabilidad y auditabilidad de la información que maneje.

- Los computadores, celulares, sistemas y otros equipos conectados a la red deben usarse solamente para las actividades propias del IMCRDZ, por lo tanto, los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que evalúe el riesgo informático de tal labor.

6.3 CONTROL DE ACCESO LOCAL A LA RED

- El responsable de sistemas o TIC´s proporcionará a los usuarios el acceso a internet para uso estrictamente laboral.

- Dado el carácter unipersonal del acceso a la Red del IMCRDZ, el responsable de sistemas o TIC´s verificará el uso responsable, acorde a las políticas de seguridad de la información.

- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, access point, switches, etc.) sean propiedad del IMCRDZ o de contratistas proveedores de Tecnología y que se encuentren conectado a la red, es administrado por el responsable de sistemas o TIC´s y puede ser ejecutado por el proveedor con el correspondiente acompañamiento.

- Todo equipo de cómputo que esté o sea conectado a la Red del IMCRDZ, debe de sujetarse a los procedimientos de acceso que emite TIC´s.

6.4 CONTROL DE ACCESO REMOTO

- El responsable de sistemas o TIC´s es el encargado de proporcionar el servicio de acceso remoto a los recursos informáticos disponibles.

- Para el caso especial de acceso al servidor de HAS dispuesto en las instalaciones del IMCRDZ por terceros, deberán ser autorizados y acompañados por el responsable de sistemas o TIC´s.

- El usuario o administrador de estos servicios deberá sujetarse al Reglamento de uso de la Red del IMCRDZ y deberá mantener concordancia con los lineamientos generales de uso de Internet.

- El acceso remoto que realicen personas ajenas al IMCRDZ deberá cumplir las normas que emite el ministerio de las TIC's.

6.5 ACCESO A LOS SISTEMAS DE INFORMACIÓN

- Tendrá acceso a la información solo el personal del IMCRDZ que tenga la previa autorización del responsable de sistemas o TIC´s.

- El manejo de información que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su seguridad.

- La instalación y uso de los sistemas de información se rigen por las normas y procedimientos establecidos por el Ministerio de las TIC´s.

6.6 ACCESO AL SISTEMA DE INFORMACIÓN FINANCIERO Y CONTABLE (HAS)

- El acceso a HAS debe solicitarse mediante una comunicación escrita al área de Tesorería con copia al responsable de sistemas o TIC´s. En dicha comunicación se debe detallar el nombre, cédula de ciudadanía y dependencia donde labora la persona a la cual se le va asignar la cuenta y debe estar firmada por el Gerente General.

- Las cuentas de usuario y claves de acceso son de uso personal e intransferible y no deben ser divulgados a ninguna persona.

- La cuenta de acceso a HAS (usuario y contraseña) son responsabilidad exclusiva de cada uno de los usuarios.

- El control de acceso a HAS será determinado de acuerdo a la unidad responsable de generar y procesar los datos involucrados.

6.7 CONTENIDO PAGINA WEB DEL IMCRDZ

- El material que aparezca en la página de Internet del IMCRDZ deberá ser aprobado por los profesionales de Prensa y según corresponda el Gerente General, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

- La información destinada a los funcionarios del IMCRDZ que se visualiza en www.imcrdz.com/funcionarios, se relaciona específicamente con el SGC de la entidad. Dicha información será aprobada por el comité de calidad previo a su publicación por parte del responsable de sistemas o TIC´s.

6.8 ACCESO FÍSICO

- Los funcionarios deben portar el carné durante su permanencia en las instalaciones.

- Los funcionarios deben reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación.

- Los funcionarios no deben permitir que personal desconocido o no autorizado entre a zonas de acceso controlado.
- No podrán salir de las instalaciones equipos de cómputo sin la respectiva autorización del responsable de sistemas o TIC´s y del Almacenista.
- Toda persona debe mostrar su maletín o bolso al guardia al ingresar o salir de las instalaciones.
- Al finalizar la relación laboral de los funcionarios o terminación de contrato, los privilegios de acceso a las instalaciones del IMCRDZ deben ser inhabilitados.
- Todo visitante debe presentar en recepción su identificación para cumplir con el procedimiento diseñado para tal fin.

7. SOFTWARE

7.1 ADQUISICIÓN DE SOFTWARE

- Del presupuesto de los proyectos que se otorga a las diferentes áreas del IMCRDZ deberá ser destinados recursos para la adquisición de software con licencia de acuerdo a lo requerido.
- El responsable de sistemas o TIC´s propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala.
- Corresponderá al responsable de sistemas o TIC´s emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

7.2 INSTALACIÓN DE SOFTWARE

- En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y acorde a la propiedad intelectual.

- El responsable de sistemas o TIC´s es el encargado de brindar asesoría y supervisión para la instalación de software informático y de telecomunicaciones.

- La instalación de software que desde el punto de vista del responsable de sistemas o TIC´s pudiera poner en riesgo los recursos del IMCRDZ no está permitida.

- Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, firewalls, privilegios de acceso, y otros que se apliquen).

- Está prohibida la instalación de software de la entidad en equipos personales que no pertenezcan al inventario tecnológico de la entidad.

7.3 ACTUALIZACIÓN DEL SOFTWARE

- Corresponde al responsable de sistemas o TIC´s autorizar o gestionar cualquier adquisición y actualización del software propiedad del IMCRDZ.

- Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por el Ministerio de las TIC´s.

7.4 AUDITORIA DE SOFTWARE INSTALADO

- El responsable de sistemas o TIC´s y Control Interno o quien haga sus veces, son los responsables de realizar revisiones periódicas para asegurar que sólo el software con licencia esté instalado en los computadores del IMCRDZ.

- El responsable de sistemas o TIC´s está autorizado para realizar auditorías en los sistemas de cómputo y sistemas de información.

7.5 SOFTWARE PROPIEDAD DEL DEPARTAMENTO IMCRDZ

- Todo el software perteneciente al IMCRDZ sea por compra, donación o cesión es propiedad del mismo y mantendrá los derechos que la ley de propiedad intelectual le confiera.

- El responsable de sistemas o TIC´s en coordinación con Almacén deberá tener un registro de todo el software propiedad del IMCRDZ.

- Todos los sistemas de software (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del IMCRDZ se mantendrán como propiedad del Instituto, respetando la propiedad intelectual del mismo.

- Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo que debe preservarse.

- Los datos, las bases de datos y los recursos informáticos del IMCRDZ deben estar resguardados.

- El responsable de sistemas o TIC´s gestionará la solicitud de patentes y derechos de creación de software propiedad del IMCRDZ en los casos que aplique.

- El responsable de sistemas o TIC´s administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política de seguridad de la información de este documento.

7.6 USO DE SOFTWARE

- Cualquier software que requiera ser instalado para trabajar en los equipos del IMCRDZ o en la red deberá ser evaluado por el responsable de sistemas o TIC´s.

- Todo el software propiedad del IMCRDZ deberá ser usado exclusivamente para asuntos relacionados con las actividades del mismo.

- Corresponde a TIC´s procurar que todo el software instalado en El IMCRDZ esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

8. CORREO ELECTRÓNICO

8.1 ASIGNACIÓN DE CUENTA DE CORREO

- La cuenta de correo electrónico asignada por la entidad debe solicitarse mediante una comunicación escrita o correo electrónico, dirigida a al responsable de sistemas o TIC´s. En dicha comunicación se debe detallar el nombre y dependencia donde labora la persona a la cual se le va asignar la cuenta.

- Las cuentas de personal administrativo de la entidad se identificarán con un dominio diferente al de los instructores así:

✓ Instructores Cultura: *area@culturazipaquira.com*
✓ Instructores Deporte: *area@deportezipaquira.com*
✓ Personal Administrativo: *area@imcrdz.com*

- Cualquier correo electrónico adicional deberá solicitarse al responsable de sistemas o TIC´s con la aprobación de Gerencia.

8.2 USO PERMITIDO

- La cuenta de correo asignada a un usuario es personal e intransferible. ***Ver anexo 1***

- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón de correo electrónico. El tener una cuenta de correo electrónico institucional compromete y obliga a cada usuario a aceptar las normas establecidas y a someterse a ellas.

- El correo es un servicio del IMCRDZ por lo que su uso es exclusivamente para actividades laborales.

- Queda estrictamente prohibido el uso del correo electrónico para propagar mensajes de tipo cadena. Si la entidad recibe quejas, denuncias o reclamaciones por estas prácticas, se tomarán las medidas pertinentes.

- Queda estrictamente prohibido el uso del correo electrónico para divulgar información confidencial del IMCRDZ.

- Queda estrictamente prohibido el uso del correo electrónico para cualquier propósito comercial, financiero, político, religioso o temas similares.

- Queda estrictamente prohibido intentar o apoderarse de claves de acceso de otros usuarios, acceder y/o modificar mensajes de otro usuario.

- Está prohibido el envío de correos con archivos adjuntos de más de 20 megas, los correos entrantes con archivos adjuntos de más de 20 megas no serán aceptados. En casos especiales se debe utilizar el servicio gratuito www.wetransfer.com. Cuando requiera enviar un archivo que exceda este tamaño, puede hacerla via **wetransfer, *como se describe en el ANEXO 2*.**

- En el caso de recibir un correo no deseado o no solicitado conocido como SPAM, este no debe ser abierto y debe ser reportado al responsable de sistemas o TIC´s.

- Toda información solicitada por la entidad al contratista o funcionario deberá ser enviada a través del correo electrónico institucional.

- Periódicamente, el administrador revisará las cuentas de correo que lleven más de 60 días sin ningún acceso. En caso tal, se procederá a su eliminación.

- La administración de las cuentas de correo electrónico es exclusiva del IMCRDZ, quien las suministra de forma gratuita para su uso institucional.

- El uso inapropiado de las cuentas de correo suministradas por el IMCRDZ, así como la violación a las políticas de uso descritas, tendrá como consecuencia la desactivación de las mismas.

- Las cuentas de correo no tendrán nombres personales, solo nombres de dependencias de la entidad ejemplo gerencia@, comunicaciones@.

- La contraseña o clave que se establece es generado automáticamente, se recomienda cambiarlo la primera vez que acceda a la plataforma de correo electrónico.

- No se pueden enviar archivos adjuntos con extensión ejecutable por lo cual no debería sorprender que se genere un mensaje automático de advertencia indicando el tema.

- Las cuentas permiten el acceso vía web, a través de la respectiva Url http://www.webnode.com y a través de programas de administración de correo

electrónico (por ejemplo: Outlook®, Thunderbird ®, etc.) la configuración de los cuales es responsabilidad del usuario.

- Una vez se cree una cuenta nueva de correo, el funcionario tendrá 15 días para acceder a ella. En caso de no presentar acceso en el plazo, será borrada automáticamente.

- En caso de necesitar creación, reinicio o cancelación de la cuenta, deberá informarse al correo sistemas@imcrdz.com o comunicarse con el responsable de Tecnologías de Información y comunicación del IMCRDZ.

- Previo a la terminación del contrato de prestación de servicios, deberá hacer entrega del correo electrónico al responsable de Tecnologías de Información y comunicación del IMCRDZ, para su respectivo paz y salvo.

8.3 BUENAS PRÁCTICAS

- Las comunicaciones realizadas a través del correo electrónico se considera una comunicación de tipo oficial.

- Se recomienda que el usuario que accede al correo vía Web, continuamente elimine aquellos mensajes que entienda no son importantes, evitando así ocupar espacio de disco duro en el servidor de correo electrónico para no afectar su rendimiento.

- Los archivos que se adjuntan en los mensajes de correo, en lo posible deben de comprimirse con el software adecuado para así evitar la degradación del servicio de correo, el consumo de ancho de banda y la saturación involuntaria de las casillas de los usuarios.

- Todos los usuarios que dispongan de correo electrónico están en la obligación de revisarlo al menos dos veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

8.4 SEGURIDAD

- Si se retira de su puesto de trabajo por un periodo de tiempo debe cerrar la sección de su cuenta de correo y bloquear su sesión de usuario, o si va a dejar de usarlo

permanentemente, cierre las aplicaciones (navegadores o clientes de correo) que esté usando y apáguelo.

- Por seguridad los archivos adjuntos con extensiones que puedan ser potenciales amenazas a la seguridad de la información no serán aceptados.

- Si sospecha que su clave de acceso ha sido violada, cambie inmediatamente la contraseña o informe inmediatamente al responsable de sistemas o TIC´s para realizar el cambio.

- La información enviada a través del correo electrónico será responsabilidad exclusiva del emisor.

8.5 ELIMINACION DE CUENTA DE CORREO

- Toda cuenta de correo electrónico será eliminada 3 días después de la notificación de retiro del funcionario o su finalización de contrato y de la entrega de la misma al responsable de sistemas o TIC´s. Será responsabilidad del funcionario realizar la copia y entrega de la información existente en el buzón a la persona designada para recibir el cargo y debe entregar copia al responsable de sistemas o TIC´s.

- Si la cuenta pasados dos meses de su creación no es utilizada, el sistema procederá a su eliminación de manera automática.

9. INTERNET

9.1 USO PERMITIDO

- El uso de Internet es exclusivamente para las actividades institucionales. El uso de Internet para asuntos personales se permite siempre y cuando su utilización sea por tiempo limitado y no esté en jornada laboral, además que esté de acuerdo con políticas del uso del Internet designado por el Ministerio de las TIC´S y no influya de manera negativa en el desempeño de las tareas y responsabilidades para con la Entidad.

- Los usuarios utilizarán únicamente los servicios para los cuales están autorizados y no deberán usar este servicio para acceder ni modificar archivos que no son de su propiedad, y mucho menos, los pertenecientes al IMCRDZ o a otras instituciones.

- Está totalmente prohibido el ingreso a páginas de contenidos sexuales, racistas o cualquier otro tipo de material ofensivo, descarga de programas que permitan realizar conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material ya sea vía Web o medios magnéticos. Los funcionarios que accidentalmente se conecten a páginas de Internet que tengan estos contenidos deben desconectarse inmediatamente e informar al responsable de sistemas o TIC´s, para que sean bloqueados.

- Está prohibido descargar música o video (a excepción de los responsables de prensa y comunicaciones), participar en juegos de entretenimiento en línea o utilizar los servicios de video, Radio y TV por demanda. Estas acciones emplean un ancho de banda considerable disminuyendo la calidad del servicio de Internet para el resto de los usuarios.

- Está prohibido la descarga, instalación y uso de programas ajenos al licenciamiento del IMCRDZ ya sea software libre (freeware o shareware), toolbars, hotbars, messenger o cualquier otra acción que altere las configuraciones ya instaladas en los computadores. Cualquier necesidad de instalar una aplicación deberá ser consultada al responsable de sistemas o TIC´s y de ser aprobada la solicitud, la instalación será llevada a cabo por él mismo.

9.2 SEGURIDAD

- Cualquier archivo descargado a través de Internet debe revisarse con un antivirus para garantizar que no contenga virus, adware, spyware o código malicioso. Estos virus pueden comprometer la seguridad del IMCRDZ, afectar el funcionamiento tanto de los computadores como del rendimiento de la red o hasta destruir la información del disco duro del computador. Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable. Todo equipo con acceso a Internet debe tener instalado un antivirus con sus bases de datos actualizadas y siempre debe estar activo.

- El nivel de seguridad del navegador de Internet debe estar configurado con un nivel medio-alto. De esta forma se controla la ejecución de secuencias de comandos, componentes, controles y complementos ActiveX provenientes de sitios de alto riesgo que puedan dañar o comprometer la información en el computador. También de esta forma se controla la descarga automática de archivos y el bloqueo de menús emergentes.

- Está prohibido hacer uso de los servicios de Internet para interferir en los sistemas de información del IMCRDZ mediante acciones deliberadas que disminuyan el desempeño o la capacidad de los equipos instalados. Así mismo y bajo ningún pretexto debe intentar burlar los esquemas de seguridad de los sistemas del IMCRDZ.

10.ESCRITORIO LIMPIO

10.1 ESCRITORIO FÍSICO

- Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos físicos o en digital, con el fin de reducir riesgos de robo de información o pérdida.

- La documentación física que esté utilizando el funcionario a manera de consulta debe estar custodiada y reposar en los cajones asignados.

- El área de archivo de cada área debe permanecer bajo llave para evitar pérdida de información.

10.2 ESCRITORIO LÓGICO

- El escritorio del equipo de Cómputo debe estar despejado y ordenado, de tal forma que la información que se encuentre en la pantalla (escritorio) del equipo sea estrictamente la requerida para la labor desempeñada.

11.GENERALES

11.1 SUPERVISIÓN Y EVALUACIÓN

- El responsable de sistemas o TIC´s podrá monitorear las actividades de los usuarios tanto en las actividades relacionadas con los sistemas de información, el uso de la red, el correo electrónico institucional y el servicio de Internet mediante estrategias de auditoria o mediante el software de control para garantizar el cumplimiento de las políticas de seguridad. De esta forma se evita cualquier riesgo a la seguridad en la operación, servicio y funcionalidad del sistema informático del IMCRDZ.

- Para efectos de que el IMCRDZ disponga de una red con alto grado de confiabilidad, se realizará un monitoreo sobre todos y cada uno de los servicios informáticos. Los sistemas considerados críticos estarán bajo monitoreo permanente y se generará a través del software de control un informe trimestral.

11.2 RESPONSABILIDADES

- Cada uno de los usuarios del IMCRDZ son responsables del cumplimiento de cada una de las políticas de seguridad y los coordinadores de las áreas deberán supervisar el cumplimiento de las mismas.

- Toda información confidencial del IMCRDZ relacionada con los sistemas de información, deberá ser tratada bajo estricta seguridad y el personal a su cargo no está autorizado a revelarlas a terceros.

- Todos los funcionarios deberán mantener el uso restringido de información confidencial, tal como información de personas naturales contemplada en la ley de habeas data y demás disposiciones.

11.3 SANCIONES

- El incumplimiento de las políticas de seguridad aquí presentadas puede acarrear consecuencias, tales como: la cancelación temporal de la cuenta de usuario del equipo de cómputo, suspensión de la cuenta de correo, bloqueo temporal del acceso al servicio de Internet; y en algunos casos, la suspensión definitiva de los accesos anteriormente mencionados.

- Otro tipo de sanciones pueden variar desde una llamada de atención, informar al usuario o hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

- En otros casos y dependiendo de la naturaleza de la acción se analizará el caso en particular y se adoptaran las medidas pertinentes

- Todas las acciones en las que se comprometa la seguridad de los sistemas informáticos del IMCRDZ y que no estén previstas en esta política, podrán ser sancionadas.
- La protección de la Información y de los Datos está contemplada en el código penal a través de la ley 1273 del 5 de enero de 2009 con la que se pretende preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones penalizando conductas inapropiadas.

CONTROL DE CAMBIOS			
Ítem ajustado	Descripción del cambio	Fecha del cambio	Versión
N.A	Creación del documento	Enero 30 de 2018	01
N.A.	Ajuste de logo IMCRDZ	Enero 21 de 2020	02
N.A.	Ajustes términos de contenido	Abril 30 de 2020	03

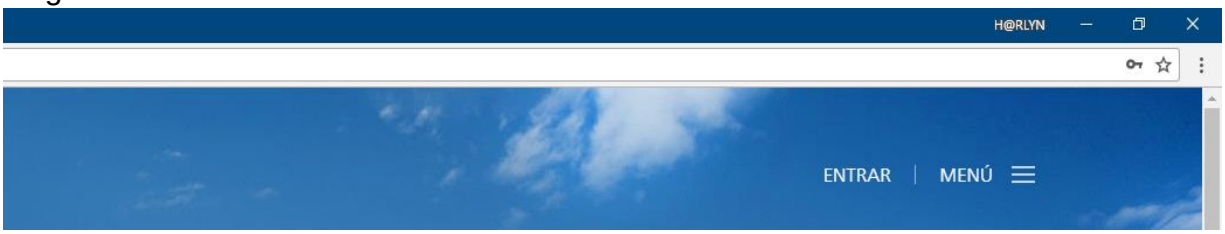
	NOMBRE	CARGO	FECHA	FIRMA
APROBÓ	Leonardo Rey Onzaga	Gerente General	Enero 30 de 2018	Se aprueba mediante acta firmada del 30 de enero de 2018. Se archiva en expediente del proceso de TIC
ELABORÓ:	Carlos Cárdenas Muñoz	Asesor SGC	Enero 20 de 2020	Se aprueba mediante acta firmada del 21 de enero de 2020. Se archiva en expediente del proceso de TIC
REVISÓ:	Oscar Mauricio Alba	Ingeniero de Sistemas	Enero 21 de 2020	
APROBÓ:	Fredy Ernesto Espinosa Cáceres	Gerente General	Enero 21 de 2020	
ELABORÓ:	Oscar Mauricio Alba	Ingeniero de Sistemas	Abril 28 de 2020	Se aprueba mediante acta firmada del 30 de abril de 2020. Se archiva en expediente del proceso de TIC
REVISÓ:	Jeimmy Lorena Olaya Forero/Carlos Cárdenas	Subgerente Administrativa y Financiera/Asesor SGC	Abril 29 de 2020	
APROBÓ:	Fredy Ernesto Espinosa Cáceres	Gerente General	Abril 30 de 2020	

12. ANEXOS

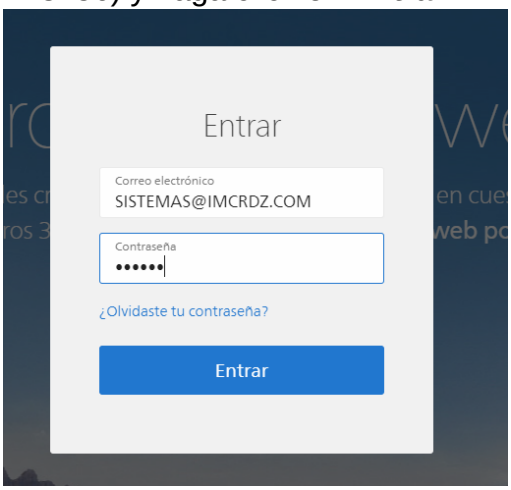
ANEXO 1
INSTRUCCIONES PARA INGRESAR A CORREO INSTITUCIONAL IMCRDZ

1. Vaya a la siguiente dirección web: www.webnode.com

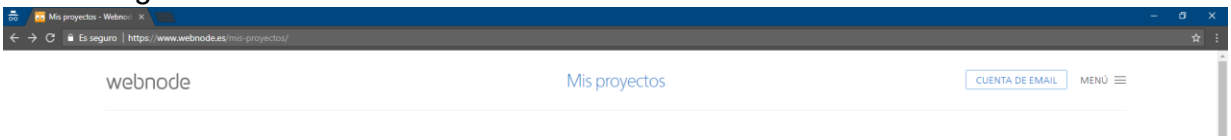
2. Haga click en **ENTRAR**



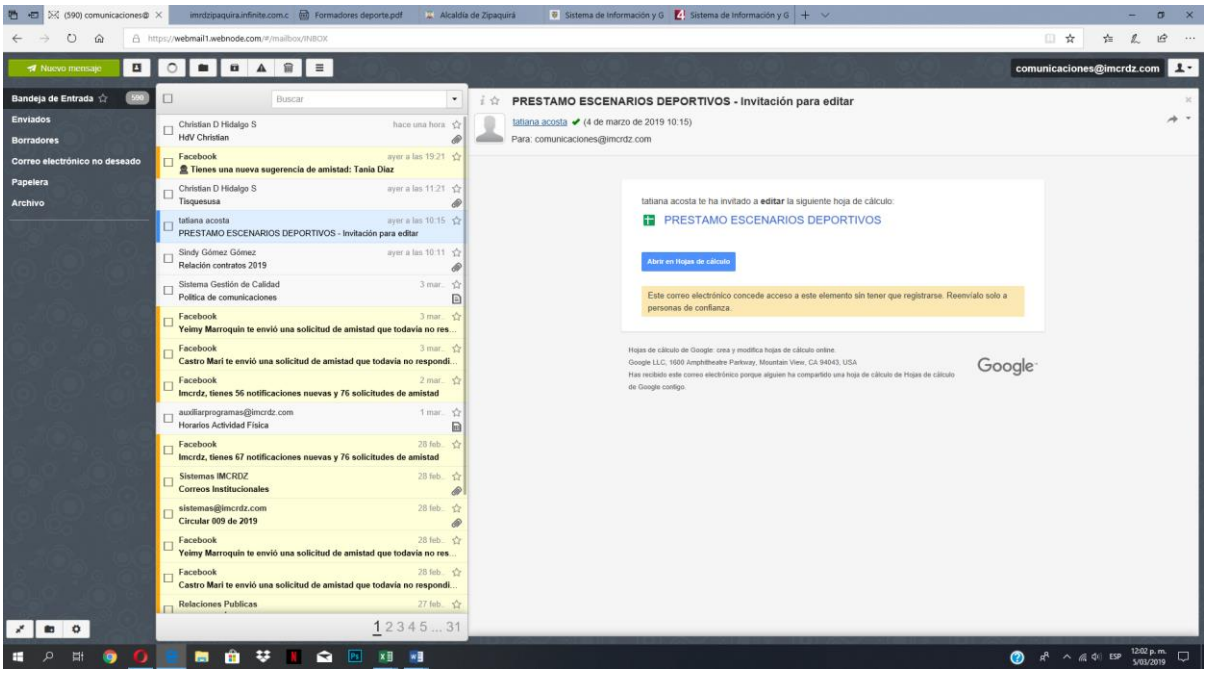
3. Digite su **correo** electrónico y la respectiva **contraseña** (contraseña inicial: 123456) y haga click en **Entrar**



4. Ahora haga click en **CUENTA DE EMAIL**



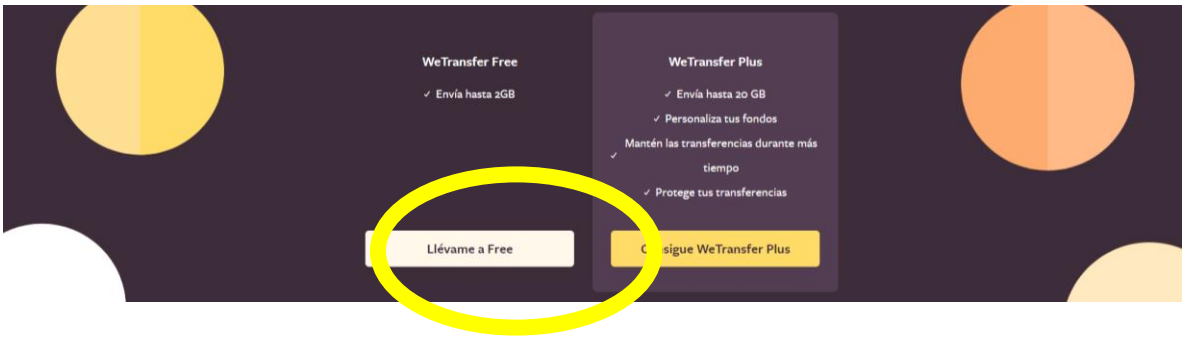
YA HA ACCEDIDO AL CORREO INSTITUCIONAL IMCRDZ



ANEXO 2
ENVÍO DE ARCHIVOS DE GRAN TAMAÑO POR WETRANSFER

1. Vaya a la siguiente dirección web: www.wetransfer.com

2. Haz click en “llévame free”



3. Da click en Añade tus archivos

4. Adjunta los archivos que se deseen enviar, con un tamaño máximo de 2 gigabytes

5. Escribe el correo o correos a quien o quienes se enviarán los archivos que hayas adjuntado, Escribe tu correo electrónico y Da Click en enviar

6. El sistema procederá a hacer el respectivo envío y enviará tanto al correo destino como al correo de envío un link donde se podrán descargar los archivos.