IOMA convos

Uso seguro de las TIC

Tecnologías de la Información y la Comunicación

Mayo 2019

Buenos Aires Provincia

INFORMACIÓN MUY IMPORTANTE

Dirección de Sistemas de Información y Estadística

Uso seguro de las Tecnologías de Información y la Comunicación (TIC) proporcionadas por IOMA

La información es un recurso vital para el funcionamiento de IOMA. La misma debe ser protegida, estableciendo diversas responsabilidades a través de mecanismos de administración y control de seguridad.

En ese marco, la Dirección de Sistemas de Información y Estadística comunica:

- IOMA es responsable de la información provista para los sectores operativos.
- IOMA designa al custodio de la misma para asegurar la disponibilidad, integridad y confidencialidad que le proveerá a la información que circule por la infraestructura informática. El custodio tiene la posesión de la información y administra técnicamente los sistemas que emplean esta información. Este rol será cumplido por la Dirección de Sistemas de Información y Estadística.
- La Dirección de Sistemas de Información y Estadística (DSIE) tiene como objetivo organizar y coordinar la infraestructura informática de telecomunicaciones y los sistemas informáticos que se utilizan en IOMA.
- La Dirección General de Administración de IOMA será responsable de la fiscalización de las políticas establecidas en este documento.

Información muy importante para agentes de IOMA

Estaciones de Trabajo (incluye computadoras, teclados, monitor, mousse, notebook)

- Se prohíbe instalar software no autorizado por IOMA. Solo un técnico de la DSIE podrá realizarlo.
- Debe solicitarse a la DSIE, por los medios correspondientes, la instalación de todo software que no esté regulado por la operatividad del área a la que pertenece el requirente. Quedará sujeto a la aprobación de la DSIE.
- Se prohíbe instalar cualquier hardware o periférico a la estación de trabajo sin coordinar con un técnico de informática.
- Para cambiar de escritorio la estación de trabajo, debe solicitarse la asistencia de la DSIE con una anticipación de 24hs.
- Toda estación de trabajo debe iniciarse con el usuario y contraseña pertinentes al agente que la utilice. Se prohíbe iniciar la misma a través de cualquier medio de almacenamiento extraíble que sirva como arranque de sistema.

- Queda prohibido el traslado de la estación de trabajo fuera del edificio.
- Los archivos utilizados por cada agente, sean compartidos o no, para utilización de cualquier otro agente de su misma repartición dentro del contexto laboral, deben estar ubicados en la carpeta compartida que será provista por la DSIE con los resguardos de seguridad que esta última proveerá.
- Cada computadora se asigna a un agente, que es el responsable de salvaguardar su integridad. Además, es el encargado de notificar a la DSIE por cualquier manipulación indebida que detecte en la misma.
- La DSIE es la encargada de llevar adelante un inventario de cada una de las estaciones de trabajo de IOMA.
- La DSIE puede remover cualquier estación de trabajo que incumpla alguna de las normas mencionadas hasta tanto regularice la situación. La DSIE notificará a la máxima autoridad del agente afectado para tomar las medidas necesarias en el marco de penalización por mal uso de las mismas.

Correo electrónico oficial de IOMA

- Al utilizar este servicio el agente representa a IOMA.
- Todo correo de IOMA debe ser solicitado por la máxima autoridad de la Dirección a la que pertenece el agente. Puede notificarse a la Dirección de Recursos Humanos, tanto las bajas, altas, como modificaciones de los mismos.
- Todas las cuentas de correo electrónico de IOMA pertenecen a un agente en particular. En caso de presentarse alguna necesidad distinta a la normativa, deberá presentar la solicitud correspondiente a la DSIE como "lista de distribución", explicando los motivos operativos por las cuales se requiere la excepción.
- Las contraseñas de cada cuenta de correo electrónico son personales e intransferibles.
- Se prohíbe el uso del correo electrónico como medio para enviar una comunicación masiva a diferentes cuentas. Para ello se contarán con casillas dedicadas para estos usos.
- La redacción de las comunicaciones para las cuentas de correos electrónicos dedicadas para este fin deben ser breves y estilo telegráficas para evitar el congestionamiento de la red. Si es imprescindible enviar un alto volumen de información, debe insertarse como documento adjunto.
- Por motivos de seguridad o rendimiento de la red, la DSIE se reserva el derecho de administrar o limitar el tráfico de archivos adjuntos u otro tipo de información anexa al servicio de correo electrónico.

Uso de internet

- El servicio de acceso a internet debe solicitarse a la DSIE por el superior jerárquico.
- El personal que no sea agente de IOMA, que se encuentre prestando un servicio y requiera acceso a Internet podrá disponer del mismo, el cual contará con las reglas de filtrado de contenido que IOMA tiene para las comunicaciones.
- Los usuarios tienen prohibido:
    - Acceder a contenido considerado inapropiado para el ámbito laboral.
    - Descargar archivos de video o audio, salvo que los mismos sean para fines laborales.
    - Realizar actividades ilegales o contrarias a los intereses de IOMA, tales como publicar información reservada, acceder sin autorización a recursos o archivos o impedir el acceso a otros usuarios mediante el mal uso deliberado de recursos comunes.
    - Efectuar actividades comerciales en Internet, excepto que lo haga en representación de IOMA mediando autorización expresa.
    - Iniciar cualquier actividad que pueda comprometer la seguridad de los servidores de IOMA.
    - Dar a conocer sus contraseñas de acceso o compartirlas con otros usuarios. La contraseña es personal y confidencial. De detectarse esta situación, el usuario quedará automáticamente inhabilitado.
    - Realizar cualquier actividad de recreación personal o de promoción de intereses personales (tales como creencias religiosas, hobbies, etc.).
    - Iniciar sesiones de Internet desde ubicaciones remotas, usando recursos de información de IOMA, excepto aquellos casos que estén debidamente autorizados por la DSIE.
    - Utilizar Internet para violar derechos de propiedad intelectual.
    - Aceptar descargas de software propuestas por páginas WEB durante su navegación.
    - Establecer una página como predeterminada diferente a la intranet de IOMA.
    - Intentar eludir los mecanismos de control y filtrado.

Monitoreo de actividades en internet

La DSIE se reserva el derecho de monitorear las actividades que realicen los usuarios en Internet. El simple uso de los servicios de Internet implica el consentimiento a este monitoreo de seguridad. Queda a criterio de cada usuario evaluar su nivel de exposición, de acuerdo con el establecimiento de sesiones que en su mayoría no son privadas.

Administración de usuarios de IOMA

- Todo agente que preste servicio dentro de IOMA y que sus funciones requieran acceso a información digital, datos, servicios, software de aplicación o software de base, debe estar acreditado con un ID de Usuario IOMA para el desempeño de las mismas.
- La solicitud debe ser realizada por el Director de la repartición a la cual pertenece el agente que requiere el ID de usuario.
- En la solicitud debe indicarse a qué servicios necesita acceder el usuario.
- Es responsabilidad del usuario final dar aviso a la DSIE en caso de que los datos considerados críticos no sean correctos o no se encuentren actualizados.
- En caso de baja, el Director del agente afectado deberá remitirse a la DSIE.
- El ID de Usuario IOMA identifica unívocamente a una persona física. Es para cada usuario, único, nominal e intransferible.
- El ID de Usuario IOMA debe tener asociado los datos de la persona responsable del mismo, de esta manera se podrá identificar de manera ágil y rápida a quién pertenece.
- Los agentes que no posean un ID de Usuario IOMA no podrán acceder a los recursos informáticos de IOMA.
- Los usuarios externos cuentan con tiempo limitado de habilitación del servicio, el cual puede ser solicitado nuevamente en caso de necesidad. Solo puede tener acceso a Internet y a las aplicaciones.
- La DSIE propicia que todos los usuarios a quienes se les habilite un ID de IOMA suscriban un compromiso de responsabilidad y confidencialidad del uso de su usuario, contraseña y de la información residente en los sistemas informáticos a los que acceda.

Contraseña

- Todo usuario que acceda a cualquier recurso informático de IOMA debe tener asociado obligatoriamente un ID y una clave de acceso o contraseña, la cual es personal, confidencial, intransferible y de exclusiva responsabilidad del usuario.
- No puede estar en blanco.

- No debe contener información personal o de fácil identificación del usuario (por ejemplo, DNI, domicilio, teléfono, fecha de nacimiento y fecha de ingreso).
- No debe ser impresa en listados del sistema, ni escrita en lugar visible a otras personas.
- Debe establecerse una longitud mínima de ocho (8) caracteres.
- Se requiere la utilización de contraseñas compuestas por la combinación de caracteres especiales, números y letras mayúsculas y minúsculas.
- Se bloqueará el usuario frente a repetidos intentos fallidos de acceso.
- Es obligatorio el cambio de usuario cuando ingrese por primera vez al sistema o servicio.
- Se solicitará el cambio obligatorio de la contraseña de forma periódica.
- La DSIE conservará un histórico de los sucesivos cambios a fin de evitar su reutilización de forma no controlada.
- Todo usuario que no haya accedido al sistema por (60) días corridos será bloqueado.
- Se debe solicitar la excepción del servicio de bloqueo por el Director del agente afectado por la inactividad que supere los días mencionados.
- Se desconectará toda sesión activa cuando la estación de trabajo no verifique uso.
- No debe utilizarse la característica de "Recordar Contraseña", en ninguna aplicación o servicio que posea esta opción.
- Cuando, por razones de ausencias prolongadas, deba reemplazarse la tarea de un usuario, no está permitido la utilización de su cuenta de identificador y clave de acceso por otra persona.
- La administración y entrega de las contraseñas de usuarios de IOMA será realizada por la DSIE.

Accesos a Software de Aplicación

- La solicitud de alta, baja o modificación de accesos debe ser realizada por el Director de la repartición a la que pertenece el usuario requirente, de acuerdo a los datos de pertenencia que posea en el padrón IOMA, a través de una nota dirigida a la DSIE.
- Las solicitudes de altas, bajas y modificaciones de accesos a software de aplicación requieren de la autorización del Propietario de la Información correspondiente, o de quien este designe.
- El Propietario de la Información solo puede aprobar o desaprobar la información recibida, no pudiendo modificar las mismas, una vez emitidas.
- La baja del ID de Usuario IOMA la realiza la DSIE.

Accesos a Recursos de Infraestructura de TIC

- El acceso y privilegios de usuarios administradores son asignados según lo que establezca el Director de la DSIE de IOMA, conforme a la necesidad que presente la Dirección del agente requirente.
- Los usuarios con acceso a los recursos de infraestructura de TIC deben ser nominales, estar identificados en el padrón IOMA y estar asociados a un ID de Usuario IOMA activo.
- Los usuarios que se encuentren identificados en el modelo de autorización de los recursos de infraestructura de TIC deben tener como identificador obligatorio y no exclusivo el CUIT/CUIL de la persona a quien pertenece el dicho ID de Usuario. Esto es para contar con una trazabilidad de actividades de usuarios que sea transversal a todo IOMA. El CUIT/CUIL debe pertenecer a personas físicas, identificadas en el padrón IOMA. No se permiten identificadores referenciales de personas jurídicas.
- No se permitirá el uso de identificadores no nominales (genéricos) para uso personal o acceso a recursos de infraestructura de TIC. Los identificadores no nominales estarán reservados para tareas de administración del sistema, usuarios por defecto de software e identificadores con privilegios funcionales críticos.
- La DSIE realizará una revisión periódica de los accesos otorgados a los usuarios en los recursos de infraestructura de TIC, a fin de identificar que los mismos sigan activos en el padrón de Usuarios IOMA. En caso de identificar usuarios cuyo ID de Usuario IOMA en el padrón haya sido deshabilitado o eliminado, se procederá a realizar la baja de los accesos a los recursos de infraestructura de TIC.