MATRIZ DE BUENAS PRÁCTICAS, VIOLACIONES Y CORRECTIVOS A LAS MISMAS

BUENAS PRÁCTICAS EN SEGURIDAD INFORMÁTICA	VIOLACIÓN DE LAS BUENAS PRÁCTICAS	CORRECTIVO
Asignar un usuario y contraseña a los funcionarios que ingresan a la compañía, de acuerdo a su perfil de actividades y a su nivel de autonomía.	Asignar permisos no congruentes con el perfil y el nivel de autonomía del funcionario.	Investigación por parte de la Gerencia de la motivación de la persona para tener más permisos de los asignados. De acuerdo a los resultados de la investigación las sanciones van desde un Memorando con copia a la hoja de vida, hasta la terminación del contrato de trabajo.
Mantener una clave de usuario confidencial, que no sea obvia y que no esté registrada en ningún lugar.	Tener una clave obvia, registrada en algún lugar y que sea conocida por más personas además del dueño de la misma.	Recordarle a la persona la forma correcta de elegir una contraseña, cambiar la que se tiene actualmente y monitorear su uso. La sanción puede llegar hasta el envío de un Memorando con copia a la hoja de vida.
Crear ó modificar información con los permisos de las personas responsables de la misma, teniendo en cuenta las consecuencias para otras áreas y procurando el bienestar de la compañía.	Crear ó modificar información sin autorización del responsable, con consecuencias para otras áreas de la compañía ó poniendo en riesgo a la misma frente a los procesos de pagos, facturación, impuestos, entre otros.	Identificar la persona que realizó la creación ó modificación de información en el sistema, recordarle el proceso correcto de creación/modificación, y hacerlo consciente de las consecuencias de sus actos. La sanción puede ir desde un llamado de atención, hasta un Memorando con copia a la hoja de vida.
Solo bajar la información autorizada por la compañía.	Bajar información no autorizada.	Ya se ha pasado un Memorado indicando que no se realice este tipo de operación. Las sanciones van desde un llamado de atención hasta un Memorando con copia a la hoja de vida.

BUENAS PRÁCTICAS EN SEGURIDAD INFORMÁTICA	VIOLACIÓN DE LAS BUENAS PRÁCTICAS	CORRECTIVO
Realizar back ups con la periodicidad indicada, con el procedimiento adecuado, dejando registro escrito del mismo y guardándolo en el lugar acordado.	- Realizar back ups sin llevar la periodicidad, el procedimiento, el registro, ni el archivo adecuado. - No realizar el back up.	- Recordarle a la persona la forma correcta de llevar el back up. La sanción es un llamado de atención. - Asignar la responsabilidad del back up a otra persona y a la que cometió la falta hacerle Memorando con copia a la hoja de vida.
Solo debe ingresar al servidor las personas autorizadas por la gerencia y por el Jefe de Sistemas.	Ingreso de personal no autorizado al servidor.	La gerencia abre investigación de la motivación de la persona para ingresar al servidor sin los permisos suficientes. De acuerdo a la investigación las sanciones van desde un Memorando con copia a la hoja de vida, hasta la terminación del contrato de trabajo.
Proteger los sistemas de información de ICSA.	Atentar contra los sistemas de información de ICSA.	La gerencia abre investigación de la motivación de la persona para atentar contra los sistemas de información de ICSA. De acuerdo a la investigación las sanciones van desde un Memorando con copia a la hoja de vida, hasta la terminación del contrato de trabajo.
Solo instalar los programas autorizados por la compañía y con su debida licencia.	Instalar programas no autorizados.	Ya se ha pasado un Memorado indicando que no se realice este tipo de operación. Las sanciones van desde un llamado de atención hasta un Memorando con copia a la hoja de vida.

ELABORADO	REVISADO	APROBADO
Paola Cardona Martínez	Paola Cardona Martínez	Lucas Cardona Martínez
Coordinadora Administrativa	Coordinadora Administrativa	
Lucas Cardona Martínez	Lucas Cardona Martínez	Jefe de Sistemas y Mantenimiento
Jefe de Sistemas	Jefe de Sistemas	
01/02/2011	15/02/2011	16/02/2011