CIRCULAR GERIES-168-2020

FUNCIONARIOS Y EMPLEADOS DE BANADESA

Conforme a lo establecido en el en el Manual de Políticas y Procedimientos de Seguridad de la Información aprobado según resolución No.JDO-011/2013; ***No.2.13 Política de Administración de Usuarios y Contraseñas***. La Gerencia de Riesgos emite la siguiente Circular la cual es de obligatorio cumplimiento.

Con el objetivo de prevenir el acceso no autorizado a la información de los sistemas del BANADESA, los usuarios deben asumir la responsabilidad sobre el manejo de su cuenta y contraseña.

Esta política señala los lineamientos necesarios para la administración de contraseñas de cualquier sistema de información utilizados para acceder a cualquier tipo de información del BANADESA. Aplicada a todo el personal permanente, empleados temporales, consultores y personal de mantenimiento que actúen en nombre y para el BANADESA.

Lineamientos sobre cuentas de usuario

Generales

a. Los usuarios son responsables de las actividades realizadas a través de su cuenta de usuario.
b. Las cuentas de usuario para recursos de cómputo deben ser utilizadas sólo por el usuario a quien fue asignada; por lo tanto, quedará estrictamente prohibido el uso compartido de cuentas de usuario.
c. Todos los usuarios deben acceder a los recursos de cómputo del BANADESA, a través de una cuenta de usuario asignada por el Área de Administración de Usuarios, con autorización del responsable de la información.
d. El correo electrónico institucional es estrictamente de uso laboral no se debe utilizar en sitios web como ser paginas de empleo, paginas de suscripciones etc.

Cambio de contraseñas

a. Cuando el usuario no pueda cambiar directamente su contraseña, debe solicitarlo al área correspondiente (Oficial de Seguridad de la Información), con el objeto de prevenir sea revelado a una entidad no autorizada.
b. Cuando se realice el cambio de contraseña, la nueva deberá ser diferente a las últimas cinco utilizadas.

Controles para las contraseñas:

a. Las contraseñas no deben ser reveladas ni compartidas, salvo en casos de emergencia, en los cuales se contará con la autorización del jefe del área. Una vez

resuelta la situación de emergencia, el responsable directo de la cuenta debe cambiar la contraseña de inmediato.

b. En caso de sospechar la revelación de una contraseña a entidades no autorizadas, deberá ser cambiada inmediatamente.
c. Las contraseñas no deben ser escritas y olvidadas en un lugar donde puedan ser del conocimiento del personal no autorizado.
d. El usuario no podrá abandonar su equipo de cómputo sin antes bloquear la sesión o apagarlo si se retira de las instalaciones del BANADESA.
e. La contraseña inicial no debe ser igual al nombre del usuario; éste tiene la responsabilidad de cambiarla inmediatamente después de su asignación y de acuerdo al formato de contraseñas válido.

Las contraseñas de usuario deben cumplir con las siguientes características:

a. Tener un mínimo de ocho caracteres.
b. Combinar letras mayúsculas, minúsculas, números y caracteres especiales, se entiende por caracteres especiales por ejemplo: #, %, $, &, etc.
f. La contraseña no debe tener información que sea fácil de averiguar, ejemplo: nombre de usuario de la cuenta, información personal como ser: cumpleaños, nombre de hijos, nombre de la mascota, nombre del esposo o esposa etc.
g. No use la misma contraseña para diferentes cuentas (ejemplo en Byte, Jteller, Zimbra etc.)
h. Evitar almacenar la contraseña en los navegadores web (Firefox, Chrome, Explorer etc.)
i. La contraseña no debe formarse con números y/o letras ejemplo: 123456, 1q2w3e, 123QWEasd
j. La contraseña no debe tener información que sea fácil de averiguar, ejemplo: nombre de usuario de la cuenta, información personal como ser: cumpleaños, nombre de hijos, nombre de la mascota, nombre del esposo o esposa, números telefónicos o fechas de nacimiento etc.
k. No se permite la repetición de contraseñas en un lapso de por lo menos, cinco asignaciones.
l. La contraseña no debe tener más de dos caracteres idénticos consecutivos.
m. La contraseña inicial no debe ser igual al nombre del usuario; éste tiene la responsabilidad de cambiarla inmediatamente después de su asignación y de acuerdo al formato de contraseñas válido.

Comayagüela M.D.C., 29 de Junio de 2020

Gerencia de Riesgos/Seguridad de la Información

C/c Jefatura de Recursos Humanos