Promipyme

PLAN DE SEGURIDAD INFORMÁTICA

CONSEJO NACIONAL PROMIPYME * Santo Domingo. R.D. * DIRECCIÓN GENERAL

Elaborado por:	Revisado por:	Aprobado por:
Soporte Técnico	Dirección de Tecnología	Dirección General
Nombre	Nombre	Nombre

Promipyme

Plan de Seguridad Informática 2022

El presente Plan de Seguridad Informática es aplicable en su totalidad a todas las dependencias de PROMIPYME. Las políticas expresadas en este plan son de cumplimiento obligatorio para todo el personal de la Institución, incluyendo al personal de las sucursales que se encuentran en todo el territorio nacional.

Políticas de Seguridad Informática de los usuarios que hacen uso de las tecnologías informáticas.

Los usuarios que hagan uso de las tecnologías propietarias de la institución son responsables de la protección de la información que utilicen o elaboren en el transcurso del desarrollo de sus labores y del uso que hagan de la misma dentro y fuera de esta entidad del estado. Todo usuario que haga uso de un recurso informático debe velar por la protección de la información apegándose a los principios de disponibilidad, confidencialidad e integridad de la misma. Esto integra desde protección del acceso a la computadora asignadas, hasta el cumplimiento del tratamiento de la información oficial que se procesa, intercambia, reproduce o conserva mediante el uso de las tecnologías de información, según su categoría y demás regulaciones.

Cada usuario tendrá acceso exclusivamente a los recursos que necesite para el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue.

Los encargados de áreas deben garantizar que la seguridad de la información sea tratada con la mayor importancia que requiera un activo institucional y que una situación que la vulnere debe ser comunicada de manera inmediata.

Las tecnologías informáticas de la institución serán utilizadas estrictamente con fines laborales

Se hará uso de herramientas que permita el respaldo/almacenamiento de la información, a fin de asegurar su disponibilidad ante cualquier situación que pueda ponerla en riesgo.

Promipyme

Todo software que vaya a ser utilizado en la institución debe cumplir con los estándares de seguridad y protección de datos establecidos por el Banco de Reservas y cumplir con el "Manual de Políticas de Seguridad Cibernética y de la Información" definidos por esta entidad. Esto es debido a que la infraestructura tecnológica utilizada por Promipyme es propietaria de esta entidad.

Está completamente prohibido el uso de dispositivos de almacenamiento como memorias USB, CD's, DVD's y cualquier otro recurso que pueda ser una vía de entrada de elementos que puedan ser perjudicial para la protección de la información o robo de la misma.

Los encargados de áreas y usuarios que hagan uso de las tecnologías de información las protegerán contra posibles hurtos, así como del robo de la información que contengan.

El movimiento de equipos informáticos debe ser solicitado a la Dirección de Tecnologia, la cual es la única área responsable a realizarlo.

En caso de recibirse documentos anexos a los mensajes se tendrá en cuenta la revisión antivirus.

El acceso al tráfico en internet es monitoreado y controlado por el Banco de Reservas. Aquellos usuarios que requieran navegar en alguna página para poder ejercer sus funciones laborales, deberá solicitar a la Dirección de Tecnologia el acceso a portal que lo requiera de manera justificada y estos se encargaran de gestionar que le sea concedida la navegación en el portal requerido.

Sistema de Seguridad Informática

No transgredir ninguna de las medidas de seguridad establecidas.

Cumplir las políticas establecidas para el empleo de las contraseñas.

No conectar ni utilizar en las computadoras ningún dispositivo de entrada o salida, ni modificar la configuración de las mismas, sin la correspondiente autorización de la Dirección de Tecnología.

Al operar el equipamiento informático y en aras de su preservación se tendrá en cuenta:

Apagarlos completamente antes de desconectarlos de la red eléctrica.

Las computadoras deberán ser apagadas al concluir la jornada laboral, salvo que por necesidades de explotación continua del sistema o de comunicaciones tengan que seguir funcionando.

En caso de ocurrencia de tormentas eléctricas severas los equipos deberán ser apagados y desconectados, salvo aquellos que por necesidad imperiosa sea requerido su funcionamiento continuo, para los cuales se tomarán medidas de protección física para mantener la integridad del equipo.

En caso de instalaciones eléctricas de alto impacto en las edificaciones de Promipyme, los equipos deben ser desconectados hasta tanto sea verificada la correcta instalación y estabilidad eléctrica.

En caso de fenómenos atmosféricos deberá desconectarse los equipos de la red eléctrica y de la red.

Mantener la limpieza de las computadoras y sus accesorios; no limpiar con paños húmedos.

Control de Acceso a los equipos Informáticos

El encargado de cada área determinará la manera en que su personal utilizará las tecnologías informáticas asignadas a su área, de forma tal que se logre un uso racional de las mismas.

Para que una persona externa tenga acceso a las tecnologías informáticas y de comunicaciones será necesario la autorización previa del Director de Tecnología y es de carácter obligatorio la presencia de un personal de tecnología durante el tiempo que dicho tercero este haciendo uso de del equipo.

Promipyme

Identificación de usuarios

A cada usuario le son asignadas credenciales para su identificación en la red, así como también para la asignación de los privilegios requeridos para la ejecución de su función en la institución.

Es obligatoria la habilitación del protector de pantalla con bloqueo de sesión para evitar que la información sea vista en momentos de inactividad y sea utilizada por intrusos.

Las contraseñas cumplirán los siguientes requisitos:

Tendrán un período de vigencia con cuotas mínimas de 1 día y máximas de 45 días de duración, no obstante, se permitirá cambiarlas fuera de estos términos de tiempos máximos y mínimos cuando las condiciones así lo exijan.

Estas deben poseer un mínimo de 8 caracteres entre los cuales serán se usó obligatorio mayúsculas, minúsculas y caracteres especiales. Tampoco será permitido el uso de una contraseña anterior hasta que no se haya realizado 24 cambios.

Está completamente prohibido que las contraseñas sean compartidas. Esto constituye una falta media por el riesgo que supone ante la suplantación de identidad, lo cual figurara en el expediente del empleado. A las tres faltas medias cometidas la institución puede prescindir del servicio del empleado infractor.

Deben ser fáciles de recordar y difícil de descifrar.

Esta determinantemente prohibido el escribir la contraseña en algún soporte físico.

Mirar bien su entorno antes de digitar la contraseña previendo que no haya personas mirando. Es una norma de buen usuario y de respeto a la privacidad no mirar el teclado de los demás mientras teclean sus contraseñas.

No enviar la contraseña por correo electrónico ni mencionarla en una conversación.

Promipyme

Prohibiciones

Está prohibida la conexión de algún equipo propiedad de terceros a la red, así como la instalación de cualquier tipo de software y de programas en las computadoras sin la autorización de la Dirección de tecnología y comunicaciones, garantizando las medidas de seguridad establecidas.

Está prohibido almacenar datos y archivos personales que contengan programas de instalación, videos, películas, fotos, audios, seriales y documentos que no estén en correspondencia con la actividad fundamental de la entidad.

Está prohibido conectar, ejecutar, distribuir o conservar en los medios de almacenamiento, programas que puedan ser utilizados para: comprobar, monitorear o transgredir la seguridad, así como información contraria al interés social, la moral y las buenas costumbres.

Cualquier situación que pueda vulnerar la seguridad de los datos y poner en riesgo la información de la institución deberá ser comunicada de inmediato a la Dirección de Tecnología de la institución, quienes darán prioridad y tomarán las medidas de lugar para erradicar la amenaza y proteger la información.