PLAN DE ACCIÓN PARA LA PROTECCIÓN DE LA INFORMACIÓN.

Procedimientos en Caso de Incidentes de Seguridad

Lo que es conocido como un incidente de seguridad es una falla en la confidencialidad, integridad o disponibilidad de la información crítica de la Dependencia.
En dado caso que llegara a suscitarse algún percance significativo en la seguridad informática, la Dirección debe proceder de la siguiente manera:

I. Se debe documentar todos los acontecimientos respecto a dicha falla, esto con el fin de poder tomar los datos registrados como evidencia futura.
II. De tal manera también es necesario documentar a detalle todas las medidas que se tomen para el restablecimiento y buen funcionamiento de las operaciones.
III. Con esto y derivado a la falla; realizar el fortalecimiento inmediato de los controles de seguridad informática a fin de evitar otro percance.

Procedimiento Aplicado para Seguridad Informática.

Al día de hoy la Dependencia cuenta con medidas de seguridad tanto para acceso y resguardo a medios Físicos e Informáticos, los cuales se desglosaran a continuación:

Normas de Seguridad para Equipos.

Esta norma aplica al acceso del personal a todos los equipos ya sean de telecomunicación de información y voz, servidores, las PC y otras estaciones de trabajo.

Normas para Identidades de Usuarios

I. Perfil de identificación única para cada usuario, administrado mediante servidor Active Directory (Directorio Activo).
II. Proporcionar derechos de acceso a sistemas específicos otorgados a ciertos usuarios, dependiendo de las necesidades del área. En casos excepcionales, la Dirección podrá autorizar identidades genéricas para identificar a grupos bien definidos de usuarios para fines específicos.
III. Habilitar a los usuarios para que cambien sus propias contraseñas, inmediatamente después de recibir su contraseña inicial, previa a su primer ingreso.
IV. Terminar la sesión y suspender los derechos de acceso del usuario tras tres intentos fallidos consecutivos de inicio de sesión.

V. Colocar el equipo en modo suspensión si las mismas permanecen inactivas por más del tiempo estipulado como tiempo máximo, requiriendo nuevamente inicio de sesión.

Normas de Controles Antivirus

Debe utilizarse un sistema estándar de detección de virus actualizado automáticamente con las siguientes características:

I. Escanear todos los archivos que ingresen en el entorno informático ya sea por email, USB o cualquier otra fuente externa; como el Internet para identificar, informar y, si se considera necesario, eliminar virus informáticos en el instante que este sea detectado por el software.
II. Derivado del escaneado de archivos y si fuera necesario, corregir o mantener en cuarentena todos los archivos que sean considerados como maliciosos.
III. Ejecutar automáticamente con regularidad el antivirus instalado en el equipo de cómputo.
IV. El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

Normas de Conexiones a Internet

Debido a la apertura de la Internet; no se puede confiar en la seguridad de la misma, por tal motivo, se debe implementar un conjunto de normas de controles de seguridad para proteger la información que se transfiere por este medio hacia nuestra red.

I. Toda conexión de equipos de cómputo a servicios de Internet deben estar justificadas por las necesidades del área y además el acceso a las mismas debe estar restringido a usuarios autorizados para fines autorizados.
II. Está prohibida la navegación en sitios de contenido que no sea justificable para el buen desempeño de las labores del Servidor Público.
III. El Departamento de redes de Datos inhabilitará todas las direcciones de Internet que cumplan con lo expuesto en el punto anterior, a medida que estas sean consultadas.
IV. Se contara con un sistema de protección de comunicaciones integrando Firewall, VPN, antivirus, filtrado Web, P2P, control IM, antispam, antiphising y calidad de servicio QoS.
V. Toda administración remota deberá realizarse a través de canales cifrados.
VI. Toda la operación de control de firewall debe contar con pruebas y monitoreo diario.

Normas de Resguardo de Información.

Para el resguardo de información crítica o relevante para la dependencia se debe realizar las siguientes actividades:

I. Realizar respaldos de seguridad periódicamente.
II. El tiempo de resguardo de la información se define en base a las necesidades del área y la criticidad del sistema, cual sea el caso.
III. Pruebas periódicas de dichos respaldos.

Administración de Redes

Todos los equipos de comunicaciones se encuentran sujetos a las mismas normas de seguridad que otros equipos y sistemas de TI de la Dependencia. Deben utilizarse controles de acceso a la red de comunicaciones y de enrutamiento de mensajes para complementar los controles implementados en el equipo conectado a las redes de comunicaciones:

I. Todas las conexiones a los sistemas de la Institución por medio de redes públicas deben ser protegidas con controles de seguridad apropiados, por ejemplo, mediante la utilización de Red Privada Virtual (VPN) y autenticación de usuarios.
II. Debe desplegarse el sistema de detección de intrusos según se considere adecuado y se justifique para detectar fallas de seguridad que afecten a las redes de comunicación.
III. Solo personal autorizado contara con el acceso al Centro de Datos, siendo restringido con el uso de Control de Accesos por medio de PIN de seguridad y confirmación de huella digital.
IV. Centro de Datos con sistema de video vigilancia 24/7.
V. Acceso al equipo mediante contraseña de usuario, tanto en el ambiente virtual como físico.

Diagrama mostrando flujo de información desde Internet hasta equipos de la dependencia y filtros de seguridad antes de llegar a ellos.