POLÍTICAS ESPECÍFICAS PARA CUMPLIMIENTO POR TODO EL PERSONAL

Para velar por la seguridad de la información en el INM, es necesario que todo el personal en la entidad se involucre, adquiera una cultura de seguridad y de obligatorio cumplimiento a estas políticas de seguridad. Esto incluye a funcionarios, contratistas, terceros, proveedores y clientes que interactúan con la información y las tecnologías del INM.

Políticas de seguridad de la información específicas para personal

Control de acceso

- Se debe velar por la confidencialidad de las credenciales de acceso a las aplicaciones del INM, así mismo de elementos de identificación para el ingreso a las instalaciones. Estos son únicos e intransferibles y no se deben entregar compartir con a nadie.
- Contraseñas:

  Las contraseñas no deben ser almacenadas en archivos de texto sin cifrar o anotadas en lugares visibles, pues se expone su confidencialidad.

  Se debe:

  - Cambiar la contraseña inicial de un sistema cuando se asigna por primera vez, por una contraseña personal. Esto también aplica para contraseñas dadas por terceros a personal del INM.
  - Cambiar periódicamente las contraseñas, ya sea cuando el sistema lo solicite o no.
  - Manejar contraseñas robustas, que cumplan con las condiciones de contraseña establecidas por el INM.

- Si se tiene a cargo algún dispositivo físico para autenticación en aplicaciones de terceros, como tokens o certificados digitales es responsabilidad de este usuario su custodia en un lugar seguro y su buen uso. No debe ser prestado, ya que su uso es personal e intransferible.

9. 6. 2. Protección de sistemas, software, equipos y redes

- Dar buen uso a los sistemas y la información, velando por la confidencialidad e integridad de ésta.

- Cuidar y proteger el equipo asignado., Debe ser para uso exclusivo de las funciones del cargo u obligaciones del contrato. En caso de pérdida, robo o daño debe reportar inmediatamente a la mesa de servicios y almacén.
- No se debe instalar software en los equipos del INM, de ser necesario, éste debe estar autorizado por la OIDT. La mesa de ayuda es la única autorizada para instalar software.
- Es prohibido el uso de software sin la correspondiente licencia.
- Bloquear la pantalla del equipo cuando no se está en el puesto de trabajo.
- Mantener el escritorio del equipo limpio. No debe haber accesos directos a documentos debido a que son susceptibles de pérdida de información, dado que no se les realiza backup.
- No dejar información confidencial clasificada en las impresoras.
- No mover equipos de cómputo, servidores o equipos de telecomunicaciones, ni conectarlos a la red, tampoco abrirlos o desarmarlos, solo OIDT está autorizada para esto. Para retirar los equipos de las instalaciones, se debe pedir la debida autorización.
- El uso de programas de diagnóstico de la red, scanners, cracking de contraseñas, etc. es restringido y usado exclusivamente por los funcionarios de OIDT, con la debida autorización.
- Está prohibido hacer uso de herramientas que evaden los controles de las redes y que comprometan la seguridad de la información o acceder por canales diferentes a los provistos por OIDT a servidores, bases de datos, equipos, sistemas de información, internet o intervenir o impedir el funcionamiento de controles y medidas de protección y seguridad de la plataforma tecnológica del INM.
- El INM permite a los contratistas el uso de sus equipos personales, si es requerido. Sin embargo, se debe tener instalado antivirus actualizado y firewall activado.

Uso del correo electrónico

- Usar el correo sólo para fines laborales. Está prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana, vayan en contravía de los derechos humanos.
- Al enviar correos masivos, el listado de cuentas debe quedar en copia oculta para evitar revelar información de cuentas de correo.

- Antes de un correo, es necesario validar que venga de una fuente confiable. Esto ayuda a minimizar el contagio de virus y códigos maliciosos. Si no está seguro de la confiabilidad del correo, no se deben abrir los adjuntos, ni links; debe reportarlo a mesa de ayuda.

Uso de Internet

- Utilizar la navegación en internet para fines laborales.
- Está prohibido ingresar a cualquier material considerado como pornográfico, ofensivo, discriminatorio o ilegal, descargar música, videos, fotos, fondos de pantalla, programas, juegos etc.
- No se debe enviar información del INM a través de correos personales o servicios de internet no autorizados.

Intercambio de información

- Utilizar los medios dispuestos por el INM para intercambio de información como son correo, chat y drive institucional.
- No está permitido el uso de USB, discos duros, DVD, SD y demás medios externos, de ser estrictamente necesario, se requiere autorización para su uso. Los dispositivos a usar deben ser de propiedad del INM y estos no deben ser conectados en equipos que no sean del INM.
- Enviar documentos definidos como activos de confidencialidad clasificada, de forma cifrada y sólo al personal autorizado.
- Dar uso a aplicaciones de chat como whatsapp o google chat, solo como medios de comunicación. La información del INM no debe transmitirse por estos medios.
- Los documentos físicos que contengan información catalogada como: pública clasificada o de uso interno, serán enviados con medidas que protejan su confidencialidad, por ejemplo, sobres cerrados.

Protección de información

- Todo el personal que maneje información que se haya especificado en la matriz de activos de información, debe velar porque dicha información esté en los repositorios definidos por el INM como son las carpetas digitales de las Tablas de Retención Documental, ya que solo allí se garantizan copias de seguridad. Esta información no debe reposar en equipo u otros dispositivos.
-
- Manejo del drive en la nube:

- Usar el espacio de almacenamiento (drive) en la nube solo con fines laborales.
- Descargar archivos del drive de nube, solo en equipos entregados o autorizados por el INM.
- Al compartir archivos, siempre se debe especificar los contactos con quién se va a compartir este, validando previamente que sean los autorizados para ver dicha información. No se debe compartir para todos.
- Los contratistas tienen la obligación de mensualmente entregar al INM la información. Cuando los contratistas se retiren del INM, es su obligación entregar toda la información y activos que tengan del INM, disponiendo la información en los repositorios establecidos y si usa equipo personal, es su deber hacer la eliminación de dicha información de éste.

Incidentes de seguridad

Reportar a la mesa de ayuda si detecta una actividad sospechosa, o si se evidencia un incidente de seguridad.

Redes sociales y medios de comunicación

- Las opiniones y expresiones que los colaboradores del INM realicen por medio de canales, medios de comunicación y redes sociales, se entenderán como puntos de vista personales que no necesariamente reflejan la posición del INM y por consiguiente la entidad descarga la responsabilidad de estás comunicaciones en su emisor.
- Los únicos autorizados para publicar información en las cuentas de redes sociales del INM son el personal de comunicaciones.
- Adicionalmente es responsabilidad del personal de comunicaciones publicar solo información categorizada como pública y no exponer datos personales.

Personal de tecnología

Si el personal labora en el área de OIDT, debe cumplir con las políticas de seguridad específicas para la gestión de las plataformas de TI y el desarrollo de software.

Políticas para proveedores

- Todo proveedor del INM, además de dar cumplimiento a las políticas específicas para personal, previamente descritas debe:

- Divulgar los requisitos de seguridad dentro de su organización y asegurar su cumplimiento a lo largo de la cadena de suministro, si contratan externamente partes del servicio.
- Si uno de sus empleados usa equipos o se conecta a la red del INM, le aplican las políticas específicas para personal, explicitas anteriormente.
- Si el proveedor maneja datos personales del personal del INM o clientes del INM, esta información debe tener los controles de seguridad necesarios para su protección.
- Si presenta un incidente de seguridad de la información que puedan afectar el servicio y/o esté en riesgo la información del INM, debe avisar en el menor tiempo posible al supervisor del INM encargado.
- Permitir al INM hacer auditorías o revisiones de seguridad de la información, en cumplimiento de sus políticas.
- Si el proveedor presta los servicios de desarrollo de software debe cumplir con los requisitos de seguridad que el supervisor le solicite dentro de los requerimientos del software.
- Una vez finalicen su contrato tienen la obligación de entregar toda la información y activos que tengan del INM. Es responsabilidad de los supervisores de contrato velar por la recepción segura de dicha información y la devolución de los activos.