POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección, aprueba las siguientes políticas de seguridad de la información, las cuales son aplicables a los servicios de Diplomados (Planeación, Inscripción y Acreditación), Maestrías y Doctorado (Planeación, Admisión e Inscripción), Proyectos Vinculados (Convenios y/o Contratos), Movilidad Académica (Estudiantil y/o Docente), apoyo en la gestión de Becas Institucionales (Investigadores y Docentes), Difusión de los Posgrados así como la Revista Computación y Sistemas, asegurando la Confiabilidad, Disponibilidad e Integridad de sus activos primarios y activos de soporte, de acuerdo a la declaración de aplicabilidad documentada en el Anexo D: Objetivos de Control y Controles de Seguridad de la Información:

1. POLÍTICA DE CONTROL DE ACCESO
2. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS
3. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO
4. POLÍTICA DE RESPALDOS
5. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN
6. POLÍTICA DE USO DE CORREO ELECTRÓNICO
7. POLÍTICA DE DESARROLLO SEGURO
8. POLÍTICA DE SEGURIDAD PARA PERSONAL VISITANTE O EXTERNO
9. POLÍTICA DE TELETRABAJO

Dr. Marco Antonio Moreno Ibarra

Director

1. POLÍTICA DE CONTROL DE ACCESO

Generales

- Todos los accesos a los equipos de telecomunicaciones administrados por el CIC son restringidos a personal ajeno, a menos que sea autorizado por el Jefe de Departamento de Soporte Técnico y Operativo (si aplica), Jefe del Departamento de Integración Tecnológica (si aplica), el Subdirector de Desarrollo Tecnológico o el Director del Centro.
- Identificar y registrar el acceso a los servicios de red y sistemas operativos o aplicaciones.
- Utilizar mecanismos de autenticación para el acceso a redes de la organización como validación por dominio o usuario y/o contraseña.
- Retirar los accesos de personal o alumnos que dejen de laborar en la organización.
- Revisar y modificar los accesos al menos cada 6 meses, después de cambios mayores o cuando se produzca un incidente de seguridad.
- Habilitar logs de actividad en cada sistema.
- Aislar los sistemas cuando se considere que la seguridad de la información está comprometida y restaurarlos cuando se verifique que no existen vulnerabilidades.
- El acceso a los videos de las cámaras de vigilancia sólo puede ser autorizado por el Subdirector de Desarrollo Tecnológico o el Director del Centro.

Acceso a red

- Para redes inalámbricas utilizar el protocolo de seguridad WPA2 o superior haciendo uso de las políticas de contraseñas seguras.
- Verificar que se cumplan las políticas institucionales de restricción de acceso o descarga de archivos en sitios peer to peer.
- Controlar el acceso a redes internas al personal interno y externo mediante medidas de aseguramiento de las contraseñas y demás mecanismos de conexión.

Acceso a sistemas operativos o aplicaciones

- Revisar los privilegios de administrador a usuarios finales y en el caso de aulas equipadas, generar cuentas de usuario normal sin privilegios de administración.
- Para la administración de aplicaciones críticas y servidores, se utilizarán cuentas distintas de acceso por usuario.
- Asegurar el uso de procedimientos de inicio seguros de sesión mediante las siguientes:
    - No se proporcionará el acceso hasta que todos los datos de entrada se hayan ingresado y validado.
    - No se proporcionarán mensajes de ayuda durante el proceso de autenticación.
    - No habrá visualización de contraseñas digitadas dentro de los sistemas.

Gestión de contraseñas

- Recomendar a los usuarios la utilización de mecanismos disuasivos para la creación de contraseñas:
    - La longitud de contraseñas debe ser de al menos 8 caracteres.
    - Utilizar combinaciones de mayúsculas, caracteres alfanuméricos y especiales (al menos uno de cada tipo).
    - Asegurar que se realice el cambio de contraseñas en el primer inicio de sesión cuando el sistema o área correspondiente haya generado la misma.
    - Recomendar que se evite el uso de palabras que sean fáciles de adivinar como: 12345, fecha de nacimiento, soporte1, etc.
- Realizar el cambio de contraseñas al menos una vez cada seis meses. Todas las cuentas tendrán esa vigencia solicitando su cambio por sistema.

Responsabilidad del usuario en el Uso de contraseñas o información secreta de autenticación

- No habilitar la función de "Recordar contraseñas".
- No compartir contraseñas.
- No guardar las contraseñas en lugares fácilmente identificables.
- Mantener secreta la información de autenticación
- Cambiar la información secreta de autenticación siempre que exista un indicio de riesgo o se cumpla la vigencia de la misma.

2. POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

Controles de cifrado:

- Cifrar los archivos word y pdf que contengan información sensible o confidencial utilizando una contraseña que se apegue a las normas correspondientes.
- Para redes inalámbricas, utilizar al menos el sistema de cifrado WPA o WPA2 "Acceso Protegido a la Red, incluido en el estándar IEEE 802.11.
- Implementar la función hash criptográfica mediante certificados para verificar la identidad de los sistemas web.
- Utilizar certificados de llaves públicas de identificación personal y protocolos SSL, funciones hash en aplicaciones web que procesen información sensible o crítica.

3. POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIO

Generales

- Mantener en orden su área de trabajo, asegurando que la información crítica o sensible se encuentre en un lugar seguro cuando se ausente del lugar asignado.
- Recoger de las impresoras los documentos con información crítica o sensible de las impresoras.
- No dejar expuesta información de uso interno, crítica o sensible cuando se reciban o encuentre cerca personal externo, sin previa autorización.
- Bloquear el equipo cuando se ausente del lugar asignado.
- Activar el protector de pantalla automática con contraseña a los 5 minutos de inactividad.
- El escritorio o pantalla del equipo no debe tener accesos o archivos con información crítica o sensible, en la medida de lo posible no debe tener accesos o archivos de uso interno.
- Evitar dejar llaves, documentos y notas con información confidencial u otro activo importante sobre el escritorio cuando se ausente del lugar asignado.
- Evitar dejar información de uso interno visible o en pizarrones cuando se retire de la oficina o salas de juntas.

4. POLÍTICA DE RESPALDOS

Generales

- Toda la información de los procesos, proyectos, servicios y clientes deberá estar respaldada en la NAS y/o en el sistema SABER.
- Para los servidores SABER y Página Web, toda la información generada deberá ser respaldada diariamente por el Departamento de Integración Tecnológica en al menos dos ubicaciones distintas. Para el caso de correo electrónico, el respaldo de usuarios y nombres de cuenta se realizará en forma bimestral.
- Cada área o usuario será responsable del respaldo de la información que generen, por lo que para los sistemas designados de respaldo de información serán responsabilidad del Departamento de Soporte Técnico y Operativo, la disponibilidad de los servicios de red y operación, así como de los accesos de los usuarios.
- En caso de pérdida de información en alguno de los sistemas web (SABER y página web) el responsable del servicio afectado, solicitará al Departamento de Integración Tecnológica, recuperar la información del último respaldo.
- Todos los procesos, proyectos y/o servicios deberán cumplir con la Política de Respaldos, con la finalidad de resguardar y controlar la información que se deriva de la operación de la organización.
- Toda la información contenida en el repositorio deberá ser considerada como confidencial.

5. POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

Transferencia de información a proveedores o clientes

- En la medida de lo posible evitar el envío de información sensible o crítica a personal externo al CIC.
- Permitir únicamente el uso de proveedores autorizados y dados de alta en el S@PBSI, para asegurar la confidencialidad de la información de uso interno, sensible o crítica cuando se envíe a personal externo al CIC.
- Hacer uso de las políticas de correo electrónico descritas en este documento.

Transferencia de información Digital o electrónica

- Entregar de manera personal la transferencia de información sensible o crítica, validando la autorización e identidad de la persona que recibirá la información.
- Definir las herramientas para el envío de información de uso interno que cuenten con mecanismos de acceso y privilegios.
- Transferencia de información utilizando mecanismos de autenticación y protocolos de cifrado o seguros previa autorización
- Proporcionar la información secreta de autenticación preferentemente de manera personal o como último recurso vía telefónica, no dejar esa información en contestadoras telefónicas ni buzones.

Transferencia de información Física

- Enviar la información de uso interno IPN con el área de mensajería, si es interna CIC realizarla de manera personal.
- Proteger la información utilizando un sobre cerrado, sin referencias sobre su contenido.

6. POLÍTICA DE USO DE CORREO ELECTRÓNICO

- Para el envío de correos electrónicos donde el contenido sea de uso exclusivo del CIC IPN, deberá efectuarse haciendo uso de un correo electrónico institucional, ya sea @cic.ipn.mx o @ipn.mx.
- Queda prohibido enviar información sensible por correo electrónico, cuentas FTP, o cualquier medio electrónico, clasificada como confidencial o que, sin serlo, el usuario no tenga atribuciones que permitan su uso y divulgación, atenten contra los derechos de autor, sea falsa, difamatoria u ofensiva.
- Queda prohibido el uso del correo electrónico para contextos diferentes al ámbito académico o función del CIC IPN, dentro y hacia afuera de la Institución.
- La generación de cuentas y su correspondiente clave de acceso, será mediante solicitud expresa del titular del área interesada dirigida al Departamento de Integración de Integración Tecnológica.
- Las cuentas de correo generadas son de carácter personal e intransferible.
- Las contraseñas pueden ser generadas por el usuario interesado en la oficina del DIT, o bien el administrador puede enviar las credenciales del correo del CIC, a una cuenta alterna proporcionada por el interesado, o bien cuando se trate de credenciales para servicios diferentes al correo electrónico, estas se envían a la correspondiente cuenta del centro.
- Los nuevos usuarios se deben ajustar a las recomendaciones señaladas en la sección referente a la Gestión de contraseñas.
- Es deber de cada usuario asegurarse de cerrar la sesión de trabajo una vez que finalice la utilización del servicio de correo correspondiente, con el fin de que nadie más pueda utilizar su identificación.
- En caso de que un usuario olvide su cuenta de correo y/o su contraseña, deberá solicitarla nuevamente en forma personal asistiendo a la oficina del Departamento de Integración Tecnológica.
- Las cuentas de correo serán eliminadas a solicitud expresa de los titulares de las áreas, o de acuerdo al cambio de estatus laboral o académico de los usuarios.

7. POLÍTICA DE DESARROLLO SEGURO

El CIC, dentro de sus políticas procura que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, asegura que todo software desarrollado o adquirido, interna o externamente cuenta con las patentes o licencias requeridas para su uso y soporte requerido.

Los sistemas de información construidos externamente o internamente deben:

- Validar la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Contar con opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Proporcionar la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros
- No divulgar información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Retirar todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como éstas no sean requeridas.
- Proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios o personas no autorizadas.
- Asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo o SQL injection.
- Adoptar para la seguridad de las webs y aplicaciones, la metodología OWASP, para las siguientes categorías:
    a) Recopilación de información: Pruebas para obtener la mayor cantidad de información posible de la aplicación/web que sirvan posteriormente para obtener información sensible o detectar ataques que vulneren la seguridad del sitio.
    b) Configuración y despliegue: Controles de seguridad en la configuración del servidor de la aplicación, la red, conexiones a la web, etc.
    c) Gestión de la Identidad: Controles de seguridad en la definición de roles, usuarios, control de cuentas y políticas de acceso en la aplicación/web.

d) Autenticación: Controles de seguridad relacionadas con el acceso a la aplicación/web como las contraseñas.
e) Autorización: Controles de seguridad para probar las posibles escaladas de privilegios o evasión de métodos de autorización en el portal. Control de la sesión: Controles de seguridad relacionados con las cookies y tiempos de sesión.
f) Validación de entrada de datos: Controles de seguridad en todas las entradas de información que disponga la aplicación/web (formularios de contacto, búsquedas, registros de información).
g) Manejo de errores: Seguridad y correcto funcionamiento de los mensajes de error que muestran las aplicaciones.
h) Criptografía: Controles para probar la seguridad y robustez de los mecanismos de cifrado que implemente la aplicación/web.
i) Lógica de la aplicación: Controles de comportamiento de la aplicación frente a usos inesperados que pueden ocasionar brechas de seguridad.
j) Pruebas de cliente: Todas las pruebas de seguridad realizadas desde el punto de vista del usuario.
k) Documentación del código fuente: Controles para comentar las diferentes partes del cuerpo de un programa, detallando las funciones, procedimientos, algoritmos; integrando además una cabecera al programa que incluya los objetivos, parámetros requeridos, banderas, condiciones de ejecución, y lo demás necesario para la claridad de interpretación del código analizado.

8. POLÍTICA DE SEGURIDAD PARA PERSONAL VISITANTE O EXTERNO

Generales

- Para toda visita externa, al menos una persona del Departamento de Soporte Técnico y Operativo o del Departamento de Integración Tecnológica, supervisará las actividades a realizarse en los sistemas previa autorización del Jefe de Departamento asociado al servicio o del Subdirector de Desarrollo Tecnológico.
- Verificar y aprobar la solicitud de entrada y salida de equipo de proveedores o personal externo autorizado para el ingreso a las instalaciones de la persona visitante.
- Otorgar el acceso siempre y cuando se tenga autorización interna para la visita.
- Verificar que el personal externo porte un gafete que lo identifique como visitante durante su estancia en las instalaciones, así como corroborar la identidad de la persona.
- No se permitirá a los proveedores hacer uso de equipo tecnológico de grabación o video dentro de las instalaciones críticas sin una autorización previa.

Acceso a la Información

- Firma de un convenio de confidencialidad y/o acuerdo de transferencia de la información por parte del proveedor.
- Cumplir con las medidas y protocolos de seguridad técnicas para la transferencia de la información.
- Retirar el acceso otorgado cuando la seguridad de la información se vea comprometida o al finalizar el periodo autorizado.

Uso de los Recursos de la Organización

El CIC, comunica las siguientes políticas al personal visitante:

- No dañar física o lógicamente los equipos o la infraestructura informática.
- No tomar fotografías o video sin previa autorización.
- No utilizar los recursos del CIC sin previa autorización.
- Evitar la descarga de programas, fotos, música, videos que no estén justificados durante su visita.
- No conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización de la Subdirección de Desarrollo Tecnológico.
- No instalar dispositivos de comunicaciones en los equipos e infraestructura tecnológica del CIC sin previo consentimiento del Jefe del DSTO o el Subdirector de Desarrollo Tecnológico.
- No realizar acciones o actividades que incumplan las leyes o regulaciones de seguridad de la información como: LFPDPPP, LPI etc.

9. POLÍTICA DE TELETRABAJO

- Deberá en su caso, de facilitar y encargarse del mantenimiento de los equipos necesarios para el trabajo, como equipo de cómputo, sillas ergonómicas, impresoras, entre otros.
- Llevar registro y control de los insumos entregados al personal que realizará trabajo en casa.
- Implementar mecanismos que preserven la seguridad de la información y datos utilizados por los empleados.
- Respetar el derecho a la desconexión del empleado al término de la jornada laboral.
- Establecer los mecanismos de capacitación y asesoría necesarios para garantizar la adaptación, aprendizaje y el uso adecuado de las tecnologías de la información de las personas trabajadoras en la modalidad de teletrabajo, con especial énfasis en aquellas que se sugiera sean realizadas en modo a distancia.
- Los trabajadores están obligados a guardar y conservar los equipos asignados, y deberán atender en general las políticas de seguridad de la información.
- El trabajador deberá atender las disposiciones de actualización de software y demás planes de mantenimiento de equipo que se lleven a cabo.