MANUAL DE RESPONSABILIDADES PARA LA SEGURIDAD FÍSICA DE LA SALA DE CÓMPUTO

Asunto:
POLITICAS Y NORMAS DE SEGURIDAD DE LA INFORMACION – SEGURIDAD FÍSICA

1. INTRODUCCIÓN

En presente documento contiene las Políticas y Normas de Seguridad de la Información relacionados con la seguridad física y del ambiente en el IMDRI. Brinda un marco de referencia para el control de acceso físico a las áreas donde se custodia o almacena información sensible, así como aquellas áreas donde se encuentren los equipos de cómputo críticos y demás infraestructura de soporte a los sistemas de información.

2. OBJETIVO

- Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información que pertenece o es custodiada por el IMDRI.

- Proteger Los Equipos de Procesamiento de información crítica del IMDRI ubicándolo en Áreas seguras y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

- Identificar y controlar los Factores de Seguridad Ambiental que Podrían Perjudicar el Normal Funcionamiento de los equipos de procesamiento de la Información de la Entidad.

3. ALCANCE

Las políticas y normas descritas en este documento aplican para todos los servidores públicos del IMDRI y terceros que ingresen a las instalaciones físicas de la entidad.

4. RESPONSABILIDAD

Las Políticas y Normas de Seguridad de la Información son de Carácter Obligatorio para todos los funcionarios y terceros vinculados con el Instituto independientemente del nivel de las tareas que desempeñe.
El Responsable de Seguridad de la Información

Definirá junto con el Responsable del proceso Gestión de Tecnologías de la Información y la Comunicación y los Responsables de Información de cada proceso de la entidad, los controles necesarios de seguridad física y ambiental para la Protección de los Activos de Información, en función a un análisis de riesgos; Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en la Presente Norma.

Líderes de Procesos del IMDRI
Definirán los niveles de acceso físico de los Funcionarios de la Entidad a las áreas restringidas bajo su responsabilidad.

Autorizarán formalmente el trabajo fuera de las instalaciones con Información de su Dependencia a los Funcionarios del Instituto cuando lo crean conveniente.

Control Interno revisará los registros de acceso de los funcionarios, Contratistas o Terceros a las instalaciones físicas, áreas seguras definidas, con el fin de verificar la eficacia de los controles físicos en la entidad.

5. POLÍTICAS Y NORMAS DE SEGURIDAD DE LA INFORMACIÓN MINISTERIO DEL INTERIOR

Políticas

Todas las áreas destinadas al procesamiento de la información según los niveles de clasificación establecidos por la entidad, (Público, Interno, Confidencial y Secreto) deben contar con protecciones físicas o perímetros de seguridad (tales como paredes, puertas de acceso controlado, recepcionistas, cámaras de seguridad), éstas deben cubrir con las necesidades en cuanto a: controles de entradas físicos, seguridad de oficinas, espacios y medios, protección contra amenazas externas y ambientales. Los controles deben ser de acuerdo a la necesidad de aseguramiento, clasificación y valoración de los activos de información establecidos por los responsables.

El IMDRI debe contar con perímetros de seguridad en las áreas donde se encuentren instalados los centros de procesamiento de la Información, Suministro de Energía Eléctrica, de Aire Acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los Sistemas de Información del Instituto.

Los Equipos de Cómputo del IMDRI deben estar protegidos frente a posibles fallas en el Suministro de Energía Eléctrica, para asegurar la continuidad del servicio.

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información del IMDRI estará protegido contra intercepción o daños.

5.1 SEGURIDAD FÍSICA Y AMBIENTAL

NORMAS

Perímetro de Seguridad Física y Ambiental:

- Los perímetros de seguridad deben estar delimitados por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción.
- Se Debe establecer y documentar claramente los perímetros de Seguridad.

- Se debe ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida. Las paredes externas del área deben ser sólidas y casi todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, (Mecanismos de control, vallas, alarmas, cerraduras, entre otras).

- Identificar claramente todas las Salidas de Emergencia en caso de escenarios catastróficos en la entidad.
- Nota: El Responsable de la Seguridad de la Información debe llevar un registro actualizado de las Áreas Seguras, donde se indique la identificación del Edificio y Área, principales Activos de información a proteger y medidas de protección física.

Controles de acceso físico

Todas las áreas destinadas al procesamiento o almacenamiento de información confidencial y secreta, así como aquellas en las que se encuentren los equipos y demás infraestructura que soporte a los sistemas de información y comunicaciones debe ser protegida con medidas de control de acceso físico tales como:

- Los Centros de Cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control con tarjetas inteligentes, sistema de alarmas o controles biométricos.

- El ingreso de terceros a los Centros de Cómputo y Centros de Cableado, debe estar debidamente registrado mediante una bitácora.

- Todos los funcionarios, Contratistas o Terceros deben portar el carnet que los acredite que prestan sus servicios al Ministerio, no deben intentar ingresar a las áreas donde no tengan la debida autorización.

Seguridad de Las Oficinas

- Los escritorios o puestos de trabajo de los servidores públicos deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información.

- Los Servidores Públicos deben colocar las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre desplegada en ellas.

- Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los funcionarios autorizados y, salvo situaciones de Emergencia, estos no deben ser transferidos a otros funcionarios de la Entidad, Contratista o Terceros con su debida autorización.

- Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

- No dejar abandonada en las impresoras información Confidencial y Secreta, una vez se haya impreso.

Protección contra Amenazas Externas y Ambientales

- Las Oficinas e instalaciones donde se procesa y/o almacena la información confidencial o secreta debe contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción automáticas de incendios.

- Se debe mantener buena ubicación de los equipos, aislado de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

- Los equipos del Centro de Cómputo deben tener control de los niveles de temperatura y humedad, estos deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada.

- Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipo que registre información, a menos que hayan sido formalmente autorizadas por el responsable del proceso involucrado y el responsable de Seguridad Información.

- No se permite comer, beber y fumar dentro de las instalaciones de procesamiento de la información del IMDRI.

Seguridad en los Servicios de Suministro Eléctrico

- Disponer de múltiples enchufes o líneas de suministro de energía eléctrica regulada.

- Contar con un Sistema de Energía Ininterrumpible UPS y/o plantas eléctricas, para asegurar el Apagado Regulado y Sistemático de los Equipos de Cómputo del IMDRI y Asegurar la continuidad de las operaciones Mientras se restablecen las fallas en el suministro de energía eléctrica.

- Se debe contar con Interruptores de Emergencias que deben estar ubicados cerca de las salidas de emergencia de las Instalaciones donde se encuentren los equipos de cómputo, con el fin de facilitar un corte rápido de la energía en caso tal se presente una situación crítica.

- El Instituto debe contar con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

- El Instituto debe contar con protección contra descargas eléctricas en los edificios donde se ubica.

Seguridad del Cableado

- Cumplir con los Requisitos Técnicos Vigentes de la República de Colombia.

- Realizar las Conexiones Adecuadas para la Energía Eléctrica y la Red De Datos.

- Proteger el Cableado de red contra Intercepción no Autorizada, el cableado debe contar con conductos como canaletas para su adecuada protección.

- El cableado Eléctrico debe estar separado del cableado de Red para Evitar posibles Interferencias.

Mantenimiento de Equipos

- Se debe dar cumplimiento al programa de mantenimiento a los equipos de la entidad.

- Se deben realizar mantenimientos preventivos y pruebas funcionales al Sistema de UPS y/o plantas eléctricas, sistemas de detección y extinción de incendios, sistemas de aire acondicionado, servidores, equipos de comunicaciones, equipos de seguridad que conforman la plataforma tecnológica del Instituto.

- Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.

- Se deben someter a las estaciones de trabajo, portátiles, servidores, equipos de comunicaciones, al mantenimiento preventivo, de acuerdo con el cronograma establecido y las especificaciones del proveedor, con la debida autorización formal del responsable del proceso Gestión de Tecnologías de la Información y la Comunicación del IMDRI.

- El Responsable del proceso Gestión de Tecnologías de la Información y la Comunicación deberá tener un Listado con las especificaciones o características de los equipos, así como también la fecha en la que cada equipo requiere actividades de mantenimiento.

- Registrar las fallas de los mantenimientos de las estaciones de trabajo, portátiles, equipos de comunicaciones y operaciones ya sean preventivo o correctivos, este tipo de registro debe indicar la fecha en la que fue realizado el mantenimiento, falla que presentó y quien realizó el mantenimiento.

Seguridad del equipo Fuera de la entidad

- El uso de equipos de cómputo, portátiles, discos removibles destinado al procesamiento de información, fuera de la instalaciones del Instituto, será autorizado por el responsable del proceso al que pertenezca el servidor público.

- El Usuario que está autorizado a retirar un equipo de cómputo o portátil debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la entidad.

- Periódicamente se debe monitorear la eficacia del control de Registros de Los Equipos, para detectar el Retiro No Autorizado de Activos de Información del Ministerio, Control que será llevado a cabo por el Líder de Seguridad de la Información.

CARLOS ANDRES ABRIL BRITO
Ingeniero de Sistemas