UBPD

UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

LINEAMIENTOS

Controles para Áreas Seguras

10 SEPTIEMBRE DE 2021

Carrera 13 No. 27 - 90 (+571) 3770607 Bogotá
www.ubpdbusquedadesaparecidos.co / servicioalciudadano@ubpdbusquedadesaparecidos.co

Anexo 1.

LINEAMIENTOS Y CONTROLES PARA ÁREAS SEGURAS

Las áreas seguras de la Entidad se determinan de acuerdo con el nivel de criticidad por la información que generan, procesan o almacenan tomando como referencia la clasificación de los activos de información donde se determina si son activos con información **Restringida**, **Privada** o **Pública**.

A continuación, se detallan los lineamientos y controles que requieren estar implementados en las áreas seguras de la Entidad.

Al determinar los factores de autenticación basados en el nivel de criticidad por la confidencialidad de la información relacionada con el área segura, se definen cuáles y cuántos niveles o factores de autenticación requieren ser implementados. Para doble factor de autenticación se combinan dos (2) de las siguientes, mientras para triple factor de autenticación (áreas con un nivel mayor de restricción), se implementarían los tres (3) tipos como se observa a continuación:

- ✔ Algo que un usuario sabe (contraseña, PIN, respuesta a una pregunta secreta, etc.)
- ✔ Algo que un usuario posee (llave, token de seguridad, tarjeta de proximidad, etc.)
- ✔ Algo que es un usuario / biometría (huella digital, iris, voz, etc.)

LINEAMIENTOS GENERALES

Las áreas seguras deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Independiente del tipo de área segura, se deben tener en cuenta los siguientes controles:

a) Los visitantes de áreas seguras deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados en la bitácora existente para este fin. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) El acceso a la información clasificada como privada o restringida y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ejemplo, tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse el registro de auditoría o los que genere cada uno de los mecanismos de autenticación de manera protegida, que permita garantizar su integridad y poder auditar todos los accesos en el momento que se requiera, La protección de estos registros se puede hacer en bases de datos cifradas, en repositorios centralizados de un SIEM, entre otras.

c) Se debe requerir que todos los servidores, contratistas o personal delegado exhiban alguna forma de identificación visible y deben asegurar que todo visitante tenga su acompañamiento y cuenten también con una identificación visible como visitante.

d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas seguras, lo cual debe ser realizado por parte del responsable o quien tenga a cargo cada una de las áreas.

e) El personal sólo debe tener conocimiento de la existencia de un área segura, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.

f) Se debe evitar el trabajo no controlado en las áreas seguras tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.

g) Las áreas seguras desocupadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.

h) El personal del servicio de soporte externo debe tener acceso limitado a las áreas seguras o a las instalaciones de procesamiento de información clasificada como privada o restringida. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

i) A menos que se autorice explícitamente de acuerdo con la solicitud de ingreso y su respectivo análisis, no debe permitirse el ingreso de equipos fotográficos, de video, audio u otro tipo de equipamiento que registre o capture información.

j) El acceso para el personal de servicios generales debe efectuarse en presencia del servidor encargado del área, o con la respectiva autorización por parte de éste, indicándole cuales son las precauciones por seguir, teniendo en cuenta el tipo de material que se encuentra en el área. Adicionalmente, debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

TIPOS DE ÁREAS SEGURAS

De acuerdo con el nivel de criticidad del área, por la información que es generada, procesada y/o almacenada, se establecen los siguientes tres tipos de áreas seguras:

1. **ARCHIVO O GESTIÓN DOCUMENTAL**
2. **CENTRO DE CÓMPUTO Y CUARTOS DE CABLEADO**
3. **OFICINAS NIVEL RESTRINGIDO**

1. ARCHIVO O GESTIÓN DOCUMENTAL

a) Se debe tener implementado un sistema de doble factor de autenticación para el ingreso a esta área.
b) Es de carácter obligatorio el contar con cámaras de seguridad que tengan alcance completo y detallado de toda el área destinada como archivo documental.
c) Se debe tener en cuenta los lineamientos para la conservación de documentos de archivos en[1]:
   - Soporte Papel:
     - En las áreas de depósito se recomienda mantener una temperatura de 15°C a 20°C con una fluctuación diaria de 4°C.
     - Se recomienda que en los depósitos de Archivo mantengan una humedad relativa entre 45% y 60% con una fluctuación diaria del 5%.
   - Fotografía:
     - Blanco y Negro: Temperatura 15 a 20 °C, con humedad relativa de 40% a 50%.
     - Color: Temperatura menor a 10°C, con humedad relativa de 25% a 35%.
   - Grabaciones:
     - Temperatura 10 a 18°C
     - Humedad relativa de 40% a 50%
   - Medios magnéticos:
     - Temperatura 14 a 10°C.
     - Humedad relativa de 40% a 50%.
   - Discos Ópticos:
     - Temperatura 16 a 20°C.
     - Humedad relativa de 35% a 45%.
   - Microfilm:
     - Temperatura 17 a 20°C.
     - Humedad relativa de 30% a 40%.
d) Se debe tener en cuenta los siguientes controles como medidas preventivas:

   - Detectores automáticos de humo o de calor conectados con servicios exteriores de urgencia.
   - Personal de vigilancia.

[1] Acuerdo N° 049 del 5 de mayo de 2000 Por el cual se desarrolla el artículo del Capítulo 7 “Conservación de Documentos” del Reglamento General de Archivos sobre “condiciones de edificios y locales destinados a archivos”.

- Sistemas de extinción escogidos con la asesoría de los bomberos: extinguidores manuales, sistemas de extinción fijos.
- Puertas cortafuego.
- Realizar programas regulares de mantenimiento de las instalaciones eléctricas y asegurarse que las salidas de emergencia sean de fácil acceso y de abertura desde el interior.
- Es necesario respetar las medidas restrictivas hacia los fumadores, aislar los productos sensibles como películas de nitrato o productos químicos inflamables y evitar las fotocopias en salas de almacenamiento o en espacios que tengan material inflamable.
- La protección contra los efectos del agua incluirá la verificación constante de los sistemas hidráulicos como canales, goteras, terrazas, ventanas, etc. Hay que asegurar el mantenimiento de las canalizaciones y evitar las redes de evacuación o suministro de agua en las placas de las salas de almacenamiento. Prever un pozo o un sistema de evacuación de aguas para las salas subterráneas.
- Se deben establecer jornadas de fumigación para evitar la presencia de plagas, insectos y roedores, y con esto evitar el deterioro biológico de la documentación.

2. CENTRO DE CÓMPUTO Y CUARTOS DE CABLEADO

a) En las instalaciones de alto riesgo se debe tener equipo de energía eléctrica no interrumpible, tanto en los equipos de red como en los servidores y demás equipos de TI.

b) En cuanto a los extintores, se debe revisar el número de estos, su capacidad, vigencia, fácil acceso y peso, garantizando sea un extintor tipo C, el cual sirve para equipos eléctricos, además deben estar debidamente demarcados los espacios donde se deberán ubicar. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso, y además que tengan un peso que sea difícil utilizarlos[2].

c) Capacitar al personal en el manejo de los equipos contra incendio y realizar las prácticas correspondientes en cuanto a su uso.

d) Con el fin de tener un respaldo para el sistema autónomo de detección y extinción de incendios, se debe contar con equipos manuales de extinción tipo C, el cual sirve para equipos eléctricos, en caso de contingencia.

[2] NFPA 10: Estándar para extintores portátiles.

e) Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente demarcadas y controladas para evitar robos por medio de estas salidas.

f) Los materiales más peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable. Por esto no se deben almacenar cintas magnéticas en los centros de cómputo.

g) Se debe tener un sistema de alimentación eléctrica regulada bajo un esquema de UPS, en caso de que el sistema principal falle, se debe contemplar tener una contingencia establecida como una planta eléctrica.

h) Se debe contar con un sistema de conexión o puesta a tierra para la protección de los equipos alojados en los centros de cómputo. Esto con el fin de proteger al personal de operación y mantenimiento, en el caso de que un bastidor del equipo tenga un alto voltaje o cuando algún cable de fase haga contacto con el bastidor accidentalmente, o debido al daño en algún componente.

i) Se debe contemplar el uso de soluciones modulares como el piso falso el cual permite realizar cambios en forma ágil y eficiente, para desplegar las instalaciones eléctricas, de datos, o controlar el flujo de aire a través del uso de rejillas. El diseño del piso y techo falso deben estar acordes con los estándares en cuanto a material, dimensiones, peso que soporta, etc.

j) Los centros de cómputo no deben estar continuos o debajo de espacios con ductos de agua, como es el caso de los baños. Esto con el fin de evitar que una fuga de líquidos afecte los equipos del área segura.

k) Los centros de cómputo no deben tener ventanas debido a que afectarían la seguridad del lugar, además también afectaría la funcionalidad y provecho del sistema de aire acondicionado.

l) Se debe contar con sistemas de aire acondicionado calculado e instalado de acuerdo con la cantidad, potencia y ubicación de los equipos, de tal manera que haya una circulación correcta tanto del aire caliente como del aire frío.

m) Los racks o gabinetes que alojan los equipos, al igual que los tableros de distribución eléctrica, deben estar siempre asegurados con llave.

n) Tanto los gabinetes, como los equipos, y el cableado, deben estar debidamente marquillados de acuerdo con los códigos definidos por la Entidad. Esto permite evitar un error o falla humana en el momento de una revisión o mantenimiento al equipo indicado.

o) Los centros de cómputo de la Entidad deben tener un sistema adecuado de iluminación que garantice su funcionalidad en todo el espacio del centro de cómputo.

p) Debe existir un sistema integral de alarmas donde se incluya el control de acceso de apertura de la puerta, así como los sistemas de detección de humo o de fuego, y los sensores de movimiento en el centro de cómputo.

q) Se debe contar con un sistema de cámaras de vigilancia, con las cuales se grabe las 24 horas del día, y con monitoreo permanente. Se debe garantizar que el sistema tenga los equipos que almacenen las grabaciones por el tiempo que defina la entidad. Esto en caso de requerirse para una investigación originada por algún evento o incidente de seguridad.

r) En cuanto a los controles ambientales, el centro de cómputo así como los cuartos de cableado deben contar con un rango aceptable de temperatura entre 20 °C y 25 °C, y el rango más adecuado de humedad debe estar entre el 40% y el 55%[3].

3. OFICINAS NIVEL RESTRINGIDO

Las oficinas catalogadas como áreas seguras son las que manejan, procesan o almacenan información **Restringida.** En estas áreas deberían:

- No existir ductos de aguas limpias o aguas servidas cerca o encima del área segura.
- Contar con puertas de seguridad resistentes a afectaciones ambientales, y a ataques externos.

En estas oficinas se deben considerar los siguientes controles:

a) Las instalaciones deben ubicarse en lugares a los cuales no pueda acceder el público de manera directa, deben ser áreas restringidas.

b) Estas áreas deben ser discretas y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información.

c) Los equipos como fotocopiadoras y máquinas de fax, deben estar ubicados adecuadamente dentro del área restringida, evitando solicitud de acceso por parte de personal de otras dependencias, el cual podría comprometer la información privada o restringida.

d) Estas áreas deben estar físicamente separadas de aquellas administradas por terceros.

[3] Norma TIA/EIA 942.

e) Las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información clasificada como privada o restringida no deben ser fácilmente accesibles al público.

f) Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área segura, es decir, que estas áreas no deben ser utilizadas como depósito ni contener elementos de material inflamable como cartón, plástico, madera, etc.

g) Estas áreas deben tener un sistema de triple factor de autenticación, de acuerdo como se mencionó al inicio del presente documento.

Proyectó: Diego Ramírez Asesor Unidad Especial/ Oficial de Seguridad de la Información/ 10/08/2021
Revisó: Diego Ramírez Asesor Unidad Especial/ Oficial de Seguridad de la Información/ 30/08/2021
Aprobó: Diego Ramírez Asesor Unidad Especial/ Oficial de Seguridad de la Información/ 10/09/2021