Contenido

VERSIONES

Versión	Elaborado por	Revisado por	Aprobado por	Fecha	Motivo
1	MERLY TORRES JAKELINE SÁNCHEZ	LAURA MARCELA PERDOMO FONSECA	COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	17/05/2022	Versión inicial

1. OBJETIVO

Prevenir daños a la información y componentes de procesamiento de información.

2. ALCANCE

Estos lineamientos deben tomarse en cuenta en todas las actividades relacionadas con el acceso a las instalaciones de RTVC y sus diferentes dependencias. Es de aplicación por parte de colaboradores y visitantes de RTVC.

3. DEFINICIONES

- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.
- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Activo de información**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- **Control**: Medidas que se implementan para modificar el riesgo.
- **Área segura:** espacio físico donde se almacena o procesa información crítica de la entidad.

4. SEGURIDAD FÍSICA Y DEL ENTORNO

4.1 Áreas seguras

4.1.1 Perímetro de seguridad física

Control: Se deben definir y usar perímetros de seguridad para proteger áreas que contengan información confidencial o crítica y las instalaciones de manejo de información.

Directrices:

- Realizar el inventario y señalizar las áreas seguras.
- El perímetro de seguridad de las instalaciones de RTVC o de las áreas seguras debe ser físicamente sólido (no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, alarmas, cerraduras, etc.
- Verificar que las puertas y ventanas de las áreas seguras estén cerradas con llave cuando no hay supervisión o están desocupadas.
- El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV (circuito cerrado de televisión) y contar con sistemas de control de acceso.
- Todas las puertas de emergencia de un perímetro de áreas seguras deben tener alarma.
- Mantener organizado e identificado el cableado en los racks de los centros de cableado y centro de datos.

4.1.2 Controles de acceso físico

Control: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.

Directrices:

- Todos los puntos de acceso a las instalaciones físicas deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico (personal interno y visitantes) a las instalaciones y debe estar documentado. Así mismo, debe contar con sistemas de control de acceso.

- El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones de RTVC.
- Registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo, servidores, equipos activos de red o cualquier equipo diferente a teléfonos; en caso de que estos equipos sean propiedad de RTVC, deberán contar con autorización expresa según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.
- Deshabilitar o modificar de manera inmediata, los privilegios de acceso físico a RTVC y a las áreas seguras, en los eventos de desvinculación o ausencia transitoria.
- Llevar el registro del acceso a las áreas seguras (centros de cómputo y centros de cableado, entre otros).
- Autorizar y acompañar el acceso al centro de cómputo, centros de cableado, gabinetes (racks) por parte de personas externas, ya que son áreas de acceso restringido donde solo debe ingresar el personal autorizado.

4.1.3 Seguridad de oficinas, recintos e instalaciones.

Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.

Directrices:

- Se debe borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas en los espacios al finalizar las reuniones.
- Garantizar que los visitantes se encuentren acompañados por un colaborador de RTVC, cuando se encuentren en las oficinas o áreas seguras donde se maneje información.
- Asegurar que los visitantes que requieran permanecer en las oficinas de RTVC por periodos superiores a dos (2) días sean presentados al personal de oficina donde permanecerán.
- Todos los colaboradores y visitantes deben portar su carné o etiqueta de visitante en un lugar visible mientras permanezca dentro de las instalaciones de RTVC.
- En ninguna circunstancia, se debe fumar, comer o beber en las áreas seguras.

- Verificar que no se toman fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de RTVC, a menos que esté autorizado.
- Verificar que las edificaciones sean discretas y no den indicio de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información.
- Verificar que las instalaciones estén configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior.
- Supervisar las actividades de limpieza en las áreas seguras, especialmente: centro de cómputo y centros de cableado, brindando capacitación al personal de limpieza acerca de las precauciones mínimas a seguir durante el proceso de limpieza. No está permitido el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.

4.1.4 Protección contra amenazas externas y ambientales

Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Directrices:

- Asegurar que los centros de cómputo o de cableado se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.
- Proveer las condiciones físicas y medioambientales necesarias como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, entre otros en los centros de cómputo y de cableado.
- Se debe garantizar el mantenimiento de los extintores contra incendios, la red contra incendios, los detectores de humo, entre otros controles que permitan la actuación en caso de emergencia.
- Mantener en buen estado la infraestructura física de los centros de cableado, centros de cómputo de RTVC, y en general de las áreas seguras, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.
- Mantener los centros de cómputo y de cableado libres de objetos o elementos

que no sean propios de la operación.
- Elaborar e implementar los planes de contingencia, de emergencia y de continuidad del negocio.

4.1.5 Trabajo en áreas seguras

Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.

Directrices:
Asegurar que las labores de mantenimiento de redes eléctricas y de datos, dentro de los centros de cómputo o cableado, sean realizadas por personal idóneo autorizado previamente por la Coordinación de T.I., así mismo, se debe llevar control de la programación de los mantenimientos preventivos y correctivos.

4.1.6 Áreas de despacho y carga

Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos donde pueden ingresar personas no autorizadas.

Directrices:
- Señalizar las áreas de carga y descarga de la entidad.
- Controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información.
- Diseñar el área de despacho y carga de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras áreas de la edificación.
- Inspeccionar y examinar el material que ingresa para determinar que no haya la presencia de explosivos, químicos u otros materiales peligrosos.

5. NORMATIVIDAD APLICABLE

ISO 27001:2013