



Agosto 2014

No 12

**BOLETÍN**

Lorenzana 710, Jardines del Bosque , Guadalajara, Jalisco.

## **DIEZ FORMAS DE GARANTIZAR LA SEGURIDAD DE LOS EMPLEADOS EN EL CENTRO DE DATOS (PARTE 1 DE 2)**

Traducido del original "[Ten ways to ensure the safety of data center employees](#)" por Andrea B. Carbajal.

Los centros de datos de hoy son mucho más grandes y consumen mucha más energía de lo que se hubiera podido imaginar solo hace unos años. Los centros de datos actuales utilizan cerca de 30 veces la energía eléctrica necesaria para operar un edificio de gobierno promedio. En total, eso requiere 80 millones de horas megawatt de energía eléctrica al año, lo que implica múltiples ocasiones de accidentes.

Las consecuencias de un accidente eléctrico en un centro de datos pueden ser severas. En los Estados Unidos, algunos estudios estiman el costo mínimo de un accidente eléctrico en 750,000 dólares. Otras consecuencias incluyen una investigación de la Agencia de Seguridad Ocupacional (*Occupational Safety and Health Administration –OSHA-*), procedimientos legales prolongados y, más trágica y significativamente, la pérdida de una vida humana.

Los propietarios y operadores de los centros de datos actuales –ya sea una agencia gubernamental o un proveedor de una agencia gubernamental- enfrentan un balance delicado. Deben caminar en la delgada línea entre garantizar la seguridad del personal, instalaciones y equipo, al mismo tiempo que mantener accesibilidad 24/7/365 para los sistemas de misión crítica. Ambos no deben ser – y de hecho no pueden ser – mutuamente excluyentes.

Hay pasos que el operador de centros de datos puede tomar desde una perspectiva de producto, sistema y políticas para minimizar el riesgo de los empleados. Aquí hay 10 actividades para mejorar la seguridad de los empleados del centro de datos.

### **#1. Desarrollar y adoptar una cultura de la seguridad**

Dada la vasta cantidad de energía eléctrica consumida por los centros de datos, la seguridad no puede ser un empleo de medio tiempo, un departamento aislado o un mero recuadro en un cuadro organizacional. En cambio, la seguridad necesita ser un compromiso de liderazgo continuo, transparente y parte de las operaciones diarias. Los centros de datos orientados hacia la seguridad crean una cultura dedicada a prácticas de trabajo seguras que afectan todo lo que se hace al interior de las paredes del centro de datos.

Idealmente, cada centro de datos debe tener dedicado un líder de seguridad, preferentemente alguien que tenga experiencia en ingeniería eléctrica, que sea responsable de todas las actividades de seguridad, incluyendo establecer y comunicar políticas fáciles de entender, desarrollar rigurosos programas de entrenamiento, conducir auditorías e inspecciones periódicas, monitorear continuamente y cumplir activamente con los cambiantes estándares y prácticas de seguridad.

### **#2. Entender la normativa relevante**

Los accidentes que involucran electricidad han tenido lugar desde que se comenzó a utilizar. Pero los centros de datos son, comparativamente, conceptos nuevos, ya que la mayoría son del dominio de los profesionales de TI más que de los ingenieros en electrónica. El mantener sistemas de energía eléctrica no es la zona de confort de la mayoría del personal del centro de datos.

Por esta razón, los operadores de centros de datos deben entender y seguir las normas críticas de seguridad para instalaciones que permiten a los empleados trabajar en equipo eléctrico. Estos estándares incluyen:

- El código eléctrico nacional NFPA 70 edición 2002.
- El estándar para los requerimientos de seguridad eléctrica FPA 70 edición 2000.
- La guía para calcular el riesgo de arco eléctrico IEEE edición estándar 1584-2002
- El código de regulaciones federales (*Code of Federal Regulations –CFR-*) OSHA 29 parte 1910 Subparte S.

Adicionalmente, la OSHA requiere que las instalaciones se adhieran estrictamente a un plan de seis puntos para minimizar y proteger a los trabajadores de incidentes por arco eléctrico:

- *Proporcionar y ser capaz de demostrar un programa de seguridad con responsabilidades definidas.*
- *Calcular el riesgo de arco eléctrico*
- *Uso correcto de equipo de protección personal (Personal Protective Equipment –PPE-) para los trabajadores*
- *Entrenar a los trabajadores en el riesgo del arco eléctrico*
- *Utilizar las herramientas apropiadas para el trabajo seguro*
- *Proporcionar las etiquetas de advertencia en el equipo*

De particular interés para los operadores de centros de datos deben ser dos secciones en particular de la norma OSHA, usualmente conocida como procedimientos de candado / etiqueta (“lockout/tagout”). La norma para el control de energía peligrosa parte 1910.147 del código de regulaciones federales provee prácticas y procedimientos claros para desmantelar maquinaria y equipo y prevenir que se libere energía peligrosa mientras los empleados llevan a cabo actividades de servicio y mantenimiento. La norma especifica medidas para controlar energías peligrosas incluyendo fuentes de energía eléctrica, mecánica, hidráulica, neumáticas, química, térmica y de otras fuentes.

Como ejemplo, el título 29 del Código de Regulaciones Federales de los Estados Unidos, en su parte 1910.147 marca requerimientos que deben cumplirse para proteger a los empleados que trabajan en circuitos eléctricos y equipo eléctrico. Esta sección requiere que los trabajadores realicen prácticas de trabajo seguras, incluyendo procedimientos de trancado y etiquetado. Estas provisiones aplican cuando los empleados están expuestos a riesgos eléctricos mientras trabajan en o ceca de conductores o sistemas que usan energía eléctrica.

Los operadores de centros de datos deben entender y atenerse a estas normas. De acuerdo a la OSHA, cumplir con estas normas previene un estimado de 120 fatalidades y 50,000 lesiones cada año.

### **#3. Observar prácticas laborales seguras**

Para todos los centros de datos, observar las normas y verificar la seguridad debe comenzar incluso antes de que las instalaciones sean construidas. Una parte crítica de cumplir con las normas de seguridad eléctrica es completar un análisis del riesgo de arco eléctrico para el sistema de distribución de energía eléctrica en las instalaciones. Este análisis es un complejo estudio de ingeniería usualmente conformado por tres partes: un estudio de corto circuito, un estudio de coordinación actual de dispositivos y un análisis de riesgo de arco eléctrico propiamente dicho.

El análisis provee un diagnóstico detallado de la energía potencial en cada punto del sistema que sería liberada en el evento de un arco eléctrico en el equipo. Basado en este análisis, el operador del centro de datos puede determinar el grado de peligro y el equipo de protección de personal apropiado que los empleados deben utilizar.

### **#4. Tener el equipo de protección personal adecuado para el trabajo**

El equipo de protección personal es la última línea de defensas contra lesiones o muerte causadas por un evento de arco eléctrico. El equipo de protección personal incluye ropa de algodón y resistente al fuego, guantes con resistencia a voltaje especificado, cascos con careta, trajes a prueba de relámpago y mantas aisladas. El equipo de protección personal es necesario siempre que un trabajador cruza la línea de protección contra arco eléctrico, pero la cantidad y el tipo de equipo de protección personal varía con el riesgo.

La determinación del nivel apropiado de equipo de protección personal se basa en el riesgo anticipado. Demasiado poco equipo de protección personal expone a un trabajador a lesiones potencialmente letales o la muerte. Mucho equipo de protección personal puede ser brumoso y puede restringir visión y movimiento, lo cual incrementa el tiempo de trabajo, la dificultad y la oportunidad de un accidente. La tabla 130.7 (C)(1)(a) de la NFPA 70E discute el uso de equipo de protección personal apropiado para todos los casos.

### **#5. Uso de etiquetas de advertencia**

Todo el equipo que puede estar sujeto a un evento de arco eléctrico debe llevar etiquetas de advertencia. Es importante entender que la responsabilidad de marcar el equipo es del operador del centro de datos, no del fabricante o instalador. Para máxima protección, las etiquetas de arco eléctrico deben llevar información adicional más allá de lo que es requerido por ley. Una calcomanía con la leyenda “Peligro. Alto voltaje”, cumple con la norma pero es demasiado genérica y puede ser ignorada. Al proveer más información en la calcomanía, los trabajadores tienen la información que necesitan para tomar decisiones informadas al seguir procedimientos de seguridad. Muchas organizaciones eligen marcar el equipo con valores específicos derivados del análisis de riesgo de arco eléctrico. Las normas actuales no requieren marcar el equipo con estos valores, pero es una buena práctica para la seguridad del área de trabajo.

*En la segunda parte de este documento se describirá cómo entender y observar áreas de trabajo seguras, tener cuidado con la electrocución, entender el riesgo de los incidentes de arco eléctrico, usar productos contra los arcos eléctricos y no ser complaciente en lo que respecta a seguridad en las prácticas del centro de datos.*