INSTITUTO ELECTORAL DEL ESTADO DE GUANAJUATO

CONTROL DE ACCESOS AL WIFI Y SEGURIDAD DE LA INFORMACIÓN

¿TE HAS PREGUNTADO POR QUÉ SE IMPLEMENTO EL NUEVO CONTROL DE ACCESO AL WIFI INSTITUCIONAL?

Anteriormente la mayoría de las personas servidoras de este instituto teníamos acceso a la wifi institucional, sin embargo, al adoptar buenas prácticas del marco de referencia **COBIT 2019** y el estándar internacional **ISO 27001** en la construcción de nuestro **modelo de gobernabilidad de las TI**, se implementaron medidas de seguridad para la protección de la información generada por el IEEG, establecidas en los **Lineamientos de Administración, Operación y de Seguridad de las TI, la Política Digital y Política de Seguridad de la Información del IEEG.**

¿CONOCES LOS RIESGOS A LOS QUE NOS ENFRENTAMOS SI NO SE CUENTA CON UN CONTROL Y USO RESPONSABLE DEL WIFI INSTITUCIONAL?

Por mencionar algunos riesgos a los que nos enfrentamos al no contar con medidas de seguridad adecuadas en el uso del wifi institucional se encuentran los relativos a:

- **Acceso no autorizado y brecha de seguridad:** esto implica que cualquier persona podría conectarse sin restricciones, lo que aumenta la probabilidad de que actores maliciosos accedan a la red.
- **Intercepción de datos sensibles:** en un organismo electoral se maneja información crítica tales como datos personales de personas servidoras, ciudadanía o incluso información relacionada con los procesos electorales. Una red sin las debidas medidas de cifrado y autenticación puede permitir que terceros intercepten y capturen estos datos, comprometiendo la confidencialidad y la integridad de la información.
- **Propagación de malware y ataques cibernéticos:** la disponibilidad de una red abierta a todo público facilita que se distribuyan virus, troyanos o ransomware a través de la conexión. Un atacante podría aprovechar la red para lanzar ataques de denegación de servicio (DoS) o incluso para infiltrar malware que se propague entre dispositivos, afectando la operatividad de los sistemas críticos del organismo.
- **Compromiso de la integridad del proceso electoral:** cualquier vulnerabilidad en la infraestructura de red podría ser explotada para interferir en la transmisión de datos relacionados con el proceso electoral. Esto no solo pone en riesgo la integridad de la información, sino que también puede generar desconfianza en el sistema electoral, afectando la credibilidad del organismo ante la ciudadanía.
- **Impacto en la imagen y confianza institucional:** En el contexto electoral, donde la transparencia y la seguridad son fundamentales, cualquier incidente relacionado con la ciberseguridad puede afectar la percepción de imparcialidad y eficiencia del organismo.



¿CÓMO SE MIDE EL RIESGO?



La fórmula "**Riesgo = Probabilidad de ocurrencia * Impacto potencial**" se considera un concepto básico y ampliamente aceptado en la gestión de riesgos, en donde:

- **Probabilidad:** Se incrementa al tener más usuarios, pues aumenta la posibilidad de que se materialicen amenazas.
- **Impacto:** Se evalúa en función de la criticidad de los activos comprometidos y de las consecuencias que tendría una brecha de seguridad (pérdida de datos, interrupción de servicios, daño reputacional).

Este enfoque se ha difundido en numerosos marcos teóricos y normativos, entre los cuales destacan:

- **ISO 31000:** La norma internacional sobre gestión de riesgos utiliza este concepto para evaluar y priorizar riesgos, definiéndolo en términos de la probabilidad de que ocurra un evento y el impacto que tendría en la organización.
- **PMBOK del PMI:** La Guía del Project Management Institute también incorpora esta idea para la evaluación de riesgos en proyectos, considerándolo una herramienta fundamental para la cuantificación y gestión de los mismos.

¿CÓMO Y CUALES SON MIS RESPONSABILIDADES PARA MINIMIZAR EL RIESGO Y PREVENIR QUE ESTOS SE MATERIALICEN?

¡¡IMPORTANTE!

Por lo anterior la Unidad Técnica de Sistemas de Información y Telecomunicaciones te invita a sumarte en la prevención del Riesgo realizando solicitudes de acceso a internet altamente responsables:

- Justifica sustanciosamente tu solicitud, ya que conforme a ello serán evaluadas en la UTSIT.
- Considera que al tener acceso al wifi contraes todas las responsabilidades dispuestas en los Lineamientos en materia de TI del IEEG por lo que cualquier incumplimiento a ello, podrás ser sujeto a las medidas administrativas correspondientes.
- Recuerda que al tener más dispositivos conectados en el área incrementa el riesgo y abres la brecha de seguridad, por lo que es importante tener en cuenta estos aspectos en el visto bueno de las solicitudes. por parte de los titulares.
- La solicitud de acceso a internet no garantiza que te sea concedido el servicio.

CONSULTA LOS LINEAMIENTOS EN:

https://api.ieeg.mx/repoinfo/Uploads/lineamientos-de-administracion-operacion-y-seguridad-ti-ieeg.pdf

Atención al art. 60 y 61 de los Lineamientos de administración, operación y seguridad de las Tecnologías de la Información del Instituto Electoral del Estado de Guanajuato