INFORME DE Auditoría

CONTROLADOR DE DOMINIO

 WINDOWS ACTIVE DIRECTORY

Informe Recomendaciones de Control Interno

30 de mayo de 2020

Señor Juan Pérez

Director de Tecnología de la Información

Estimado:

En la ejecución de nuestros procedimientos de auditoría interna, acerca de la auditoría realizada al Controlador de Dominio, evaluamos el control interno con el propósito de expresar nuestras conclusiones sobre dicha plataforma y no para proporcionar una garantía sobre el control interno, sin embargo, detectamos algunos asuntos que involucran el control interno y su operación que consideramos son condiciones para informar bajo el Marco Internacional para la práctica de la Profesión de Auditoría Interna. Las condiciones para informar involucran asuntos que llaman nuestra atención relacionados con oportunidades de mejora en el diseño u operación del control interno que, podrían afectar en forma adversa la empresa para iniciar, registrar, procesar e informar datos financieros.

Esta auditoria fue realizada al corte del 31 de diciembre de 2019. Su alcance consistió en evaluar los parámetros de configuración del Servidor Controlador de Dominio para validar que están acorde a las mejores prácticas de seguridad.

Los hallazgos y recomendaciones enumeradas en este documento, los cuales resultaron de nuestra consideración del control interno y la revisión de las diferentes evidencias obtenidas, se presentan para su conocimiento con el propósito de asistir a la administración, en el mejoramiento de sus procedimientos y controles.

A continuación, presentamos un resumen de las principales oportunidades de mejoras y su impacto sobre el control interno de la empresa.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Hallazgo identificado**  | **Impacto** **Alto** | **Impacto** **Medio** | **Impacto** **Bajo** |
| 1 | Debilidad en la configuración del parámetro sobre registro de eventos de auditoría. |  | X |  |
| 2 | Vulnerabilidad de seguridad en configuración de parámetros bloqueo de cuentas de usuarios. | X |  |  |

**Hallazgos**

|  |
| --- |
| **Recomendación de Auditoría Interna** |
| **Nombre del departamento (Unidad Auditada):**Departamento de Tecnología de la Información.  |
|
| ***Hallazgo No. 01*** | Debilidad en la configuración del parámetro sobre registros de eventos de auditoría. |
|
|
| ***Observaciones:***Como resultado de la evaluación realizada sobre la configuración y parámetros de seguridad del servidor Controlador de Dominio identificamos que la opción “Audit Account Logon Events” que determina si serán registrados los eventos de inicio de sesión de las cuentas de usuarios, no está habilitada de acuerdo a lo sugerido por las mejores prácticas de seguridad.“Ver más detalles de esto en el anexo “Evidencia-1”.  |
| ***Riesgos de mayor impacto:***Accesos no autorizados a los sistemas de la empresa a través de ataques de fuerza bruta que no fueron detectados.Dificulta realizar de forma efectiva las actividades de monitoreo de seguridad.Se pudieran ejecutar actividades no autorizadas sin dejar rastros. |
| ***Recomendación:***Evaluar activar el parámetro “Audit Account Logon Events” de manera que sean registrados los intentos de inicio de sesión fallidos de los usuarios. |
| **Comentarios de la administración y plan de acción:**  | Responsable: | Plazo de cumplimiento: |

|  |
| --- |
| **Recomendación de Auditoría Interna** |
| **Nombre del departamento (Unidad Auditada):**Departamento de Tecnología de la Información.  |
| ***Hallazgo No. 02*** | Vulnerabilidad de seguridad en configuración de parámetros sobre bloqueo de cuentas de usuarios. |
| ***Observaciones:***Como resultado de la evaluación realizada sobre la configuración de los parámetros de seguridad de las cuentas de usuarios, identificamos que no está definida la opción “*Account Lockout Duration”* que determina la cantidad de minutos que una cuenta bloqueada permanecerá bloqueada antes de que se desbloquee automáticamente y el parámetro *“Account Lockout Threshold”* quedetermina el número de intentos de inicio de sesión fallidos que harán que una cuenta de usuario se bloquee. Está configurado con valor cero lo que indica que las cuentas de usuario no se bloquean por intentos de accesos fallidos lo que no está configurado de acuerdo a las mejores prácticas de seguridad sugeridas por el fabricante Microsoft.“Ver más detalles de esto en el anexo “Evidencia-2”. |
| ***Riesgos de mayor impacto:***Accesos no autorizados a los sistemas de la empresa a través de ataques de fuerza bruta.La disponibilidad, integridad y confidencialidad de la información puede verse comprometida por software maliciosos que logran escalar privilegios en los sistemas. |
| ***Recomendación:***Evaluar activar el parámetro “Audit Account Logon Events” de manera que sean registrados los intentos de inicio de sesión fallidos. |
| **Comentarios de la administración y plan de acción:**  | Responsable: | Plazo de cumplimiento: |

Agradecemos a la Administración por la colaboración y cortesía mostradas durante nuestro trabajo.

Atentamente,

David Amarante

Dirección de Auditoría Interna